International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

An Efficient Rushing Attack Prevention Algorithm for MANET Using Random Route Selection

Aakanksha Jain[1], Samidha Dwivedi Sharma[2]

[1]NRI Institute of Information Science & Technology Bhopal, Madhya Pradesh, India

[2]Head of the Department, Department of Information Technology
NRI Institute of Information Science & Technology Bhopal, Madhya Pradesh, India

Abstract: ***Rushing attacks in mobile ad hoc networks (MANETs) cause system resources to become scarce and isolates legitimate users from the network because of this data received by the destination is not reliable. Therefore, this sort of attack significantly influences network connectivity and weakens networking functions and capabilities such as control data integrity and message delivery. This paper will focus on rushing attack which threatens the security of the mobile ad hoc network by analyzing this type of attack and its impact on mobile ad hoc networks. First, previous research on rushing attack is examined as well as the various protocols established to improve the best solution for this attack. Second, we analyze the DSR and Secured Dynamic Source Routing (SDSR) protocol which has been designed to address rushing attack, to reduce overhead in the network and the time required. Furthermore, we highlight the drawbacks and strengths of the Secured Dynamic Source Routing protocol, and find that this is the best solution to address the rushing attack problem. In addition, this thesis proposes two algorithms to reduce the overhead and time in the DSR and SDSR protocol to ensure all neighbors in the network are receiving safe data. Finally, this work concludes by summarizing the major achievements of this research and discusses future work***.

Keywords: Ad hoc networks, Rushing attacks, DSR, SDSR, Denial of service, Random Route Selection, Average time, MANET.

1. Introduction

The communications era has developed greatly over the last few centuries. It began in 1893 with Nikola Tesla, when the first successful wireless information Transmission was executed. Although this was an important breakthrough in wireless communications, it was not possible to progress this development until the last part of the twentieth century. With the demanding use of mobile phone technology, wireless communication became more important. As a consequence, the advantages of wireless communications which include reducing the infrastructure requirements and encouraging mobile networks, motivated communications researchers to search for a new network which uses a Cellular system without depending on fixed infrastructure, which led to the development of mobile ad hoc networks. Mobile ad hoc networks (MANETs) can be defined as a network where the nodes are mobile and can connect to each other through wireless communication without relying on any fixed infrastructure. The advantages of MANETs have been utilized in many different applications and by many different user groups, for example, in military applications where wireless communication is an advantage; in emergency situations such as flood, fire and earthquake to facilitate communication to deploy and direct rescue and emergency services personnel; in business or workplace applications such as video conferencing and in civilian applications such as communication between taxis. Nowadays, the growth of Wi-Fi and laptops has made MANETs a popular and important research topic for development of our nation and world, more than ever before. However, there are many challenges facing MANETs, such as power, unreliable physical channels, range limitations and half of the dual wireless without the support of any infrastructure. On the other hand, there are many advantages for using these networks, for example, self infrastructure, reduced cost, speed of deployment, etc. This paper attempts to provide an efficient method using random route selection to reduce rushing attack problem in MANETs and it will highlight some of the research that has been done in the security area, and analyses the types of security threats facing these networks. Particularly, it analyses rushing attack, how it happens and possible best solutions to prevent this from the related works.

2. Related Work

Some of the previous work on secure routing protocols such as SAODV, ARAN, ARIADNE, and SRP will be discussed in this section and compared to the SDSR protocol.

2.1 Secure Ad Hoc On-Demand Distance Vector Protocol (SAODV)

This protocol is an extension of the Ad hoc On-demand Distance Vector protocol. In addition, it suggests a pre-established public key infrastructure which hands out signed public keys to other nodes in the network. Thus, those nodes can verify signatures or encrypt the traffic to other nodes. Because of using the private key of the source via a signature, all static sections of RREQ or RREP are protected from any alteration. What is more, the mutable part and the hop count are protected by using hash chains, otherwise attackers can cut or shorten routes or increase their length. The source of the packet can compute the hash chain by using the hash function and a random number as a begging value (seed). After this, the result which is called the top hash and (seed) are saved in the packet. All the nodes that forward the packet compute a new hash chain as well as increase the hop count, which can be done via doing the

hash function to the hash value in the packet or request. Therefore, all nodes can now verify whether the hop count and the place in the hash chain is the same or not. However, rejecting unwanted traffic is still possible through increasing the hop count by an arbitrary number.

2.2 Secure Remote Password Protocol (SRP)

The Secure Routing Protocol assumes that the source and destination can share a symmetric key which is considered a light-weight solution. This solution suggests that the data can be protected via message authentication codes which are known as MACs. Although there is extremely low overhead, the intermediary nodes can be noted unauthenticated therefore, the network may face numerous potential attacks. In addition, it is unknown in this protocol how the keys should be exchanged without established routes.

2.3 ARIADNE

This protocol is based on DSR as well, but it applies hash chains to protect routing messages. This protocol is based on three modes of operation:

1. Pre-established symmetric keys.
2. Digital signatures.
3. Saving broadcast messages via the TESLA system.

In this protocol, the destination knows the source identity via the source of the route discovery request and is able to authenticate all other nodes, so this can prevent route shortening through per-hop hashing. As a result, all tasks are achieved with less use of asymmetric cryptography. However, it is unclear how some of the requirements such as distributed symmetric keys and synchronized clocks will be realized.

2.4 Authenticated Routing Protocol (ARAN)

Authenticated Routing for Ad hoc Networks uses asymmetric cryptography key pairs such as SAODV via the signed public keys which are available to all the nodes in the network. In this protocol, all nodes that forward the packet have to sign it and check the signatures which protect all routing data. As the route discovery in the ARAN protocol does not support a TTL field or a hop count, there will not be any modifying parts in the packet and the static signatures are considered sufficient. However, it was noted that the overhead in the network is huge because of the flooding of the route discovery packets are unable to be controlled. In addition, with ARAN, the problem of route lengthening is possible.

3. Existing Security Threats in MANET

Security in mobile ad hoc networks can be defined as the protection of the communications between the mobile nodes in the communications environment. Compared with wire line networks, the unrivalled features of mobile ad hoc networks create a number of problems to security design, such as a highly dynamic network topology, stringent resource constraints, peer-to-peer network architecture and a shared wireless medium. Although mobile ad hoc networks (MANETs) offer huge advantages such as easy of deployment, speed of deployment and decreased dependence on infrastructure, security is a primary concern to system security designers for many reasons. First, wireless networks are considered very vulnerable “to attacks ranging from passive eavesdropping to active interfering”. Second, security 2011 Third International Conference on Intelligent Networking and Collaborative Systems mechanisms face some difficulties in communicating due to the lack of a Trusted Third Party (TTP) or an online Certificate Authority (CA). Third, due to power limitations and computation capabilities, mobile devices are more susceptible to Denial of Service attacks (DoS) and are unable to perform computation-heavy algorithms such as public key algorithms. Fourth, adversaries can use trusted nodes to attack the network. In other words, it is more important to protect the network from inside attacks than outside attacks because these are more difficult to detect. Finally, the movement of the mobile nodes creates difficulties in detecting old routing information and false routing information. Therefore, security should encompass a number of features that must be addressed such as confidentiality, availability, authentication, integrity and non-repudiation. Malicious nodes can easily impact the correct functions of DSR by fabricating routing details, impersonating other nodes to disrupt availability, confidentiality and integrity.

The following are considered common ways to attack DSR:

- The RREQ, RREP and ERR can be forwarded, modified, fabricated or impersonated incorrectly.
- Delete ERR message to prevent searching for other routes.
- The attacks can be replayed.
- Overload via sending route control messages or forming loops which can causes DoS (denial of service).
- Salvage a correct route instead of failed route.
- Cause route cache poisoning, which is classified as a passive attack against route integrity (24).
- An illegitimate node can be used to eavesdrop on the traffic destined for another device or node.
- A tunneling attack can be implemented by conspiracy to pull traffic to object packets or collect information.
- The protocol performance may be degraded via lengthening the path.

4. Description of the Secured Dynamic Source Routing Protocol (SDSR)

In order to reduce overhead in the network, instead of forwarding all packets or route requests, existing on demand routing protocols forward the first packet and then discard the rest. Unfortunately, this can assist rushing attack, as explained in the previous paper. The network shown in Figure 1 describes how rushing attack can occur via this function.

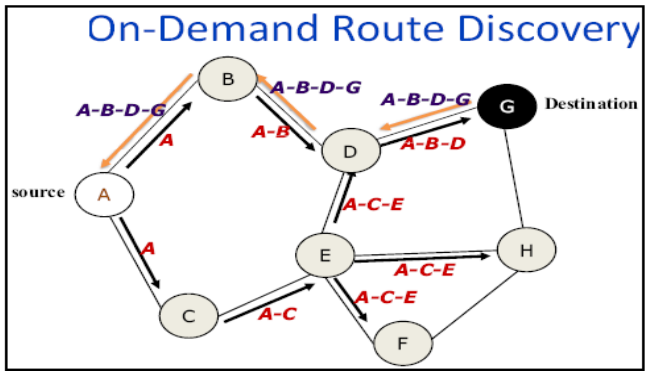

Figure 1: Route request (broadcasting request)

As shown in this figure, when the source node A initiates the RREQ to the destination node G, if the RREQs is forwarded by a malicious node which in this example is supposed to be node B, all the RREQs that come from node B will reach the destination earlier than any RREQs that are forwarded by other nodes, as shown in Figure 1.

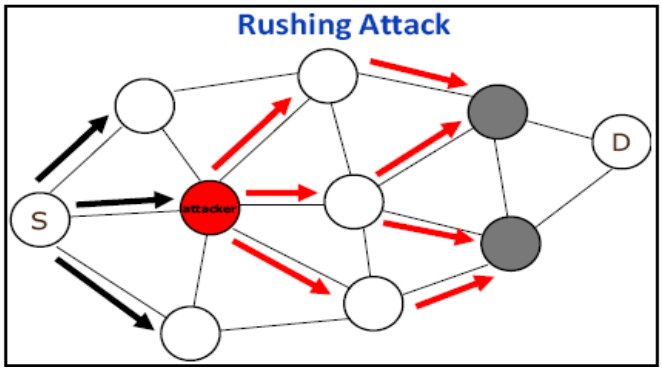

Figure 2: Rushing Request

As shown above, all the legitimate RREQs cannot reach the destination before the attacker's RREQs. Therefore, the network will be exposed to the security risks from rushing attack. As a result of this risk, this property needs to be changed to protect networks from this kind of attack. SDSR, which is based on the DSR protocol functionality, has been shown to successfully address this problem. In SDSR, instead of forwarding the first RREQ when it arrives, which could have been sent by the attacker, every node waits for a particular time before forwarding the RREQs according to the algorithm of SDSR.

5. Drawback in DSR and SDSR Algorithm

5.1 Existing problem in DSR algorithm

According to the study in the DSR Algorithm when packets send from source to destination its forward number of packets but this protocol accept only first packet and select the path to reach the destination to reduce the overhead , denial of service , eavesdropping and delay. Because of this algorithm rushing attack can occur easily we can analysis that if first node is malicious node and then the path selected for data transmission will be unbelievable. Following are the problem can occur via this problem.

- We can loss confidentiality of the data.
- Packet dropping.
- Integrity of data will not be there.

5.2 Existing problem with SDSR Algorithm

According to the study in the SDSR algorithm this is developed to overcome the shortcoming of the DSR algorithm. In the SDSR algorithm node wait for the particular time and then forward the packet so that the problem in the DSR can be short out. Further we can analysis that if eavesdropping occurs the malicious node will keep the packet for particular time and then forward the packet. By the result of this rushing attack can occur again and node can be isolate. The above drawback can occurs again.

6. Proposed Solution

Here to overcome the shortcoming of the DSR and SDSR algorithm we are proposing algorithm which based on the random route selection. This algorithm time based. For example anyone want to send data from source S to destination D adjacent for node S are C , B , D , E and time to reach these node from source are t1,t2,t3,t4 respectively. If we assume t1 is smaller and t4 is highest then According to DSR algorithm C node first receive the data and make the path for data transmission. Further we take SDSR algorithm according to which packet will wait for the particular and the data transmission will start. According to our propose algorithm we do not fixed the path for data transmission. The first solution, our algorithm will select the random path for every time data transmission so that the malicious node cannot continue to harm our data. Second, our algorithm will calculate the average travel time from source to the adjacent node. As state above t1, t2, t3 and t4 are travel time from source to adjacent node.

Tavg = (t1+t2+t3+t4)/4

If any packet which is taking time less than Tavg the node will discard all the packets. As per our algorithm all the packet which received after taking at least Tavg time that packet will only be acceptable.

7. Conclusion

As an introduction to the work in this thesis, basic information about the features and applications of ad hoc networks and rushing attack was given. The issue of security, confidentiality and data integrity in mobile ad hoc networks was addressed by examining various previous important routing protocols such as AODV, DSDV, and DSR. Different types of attacks which threaten MANETs were overviewed, for example, modification, impersonation, fabrication, wormhole and the lack of cooperation. Previous work in the area of rushing attack was explained and described, along with the solutions that can assist in preventing rushing attack. This paper proposed the best solution in detail for preventing rushing attack in mobile ad hoc networks, SDSR and DSR developed to improve security in this network, with two important goals in mind.

- To lower overhead
- To ensure there are safe neighbors in the network.

This thesis proposed two solutions: firstly, to reduce overhead by using the DSR algorithm and secondly, the message that received by the destination node itself to determine the safest and fastest route. Finally, in the proposed future work, our aim to further develops the security of Mobile Ad hoc Networks was outlined. In future work, we will try to implement this solution on other attacks to see the results that can be achieved with this protocol. Furthermore, other weaknesses of this protocol will be addressed in order to improve it.

References

[1] Tavli, B. and W. Heinzelman, "Mobile Ad Hoc Networks:Energy-Efficient Real-Time Data Communications ". 2006: Springer.
[2] Hu, Y., A. Perrig, and D. Johnson. "Efficient security mechanisms for routing protocols." 2003: Citeseer.
[3] Capkun, S., J. Hubaux, and L. Buttyan, "Mobility helps peer-to-peer security". IEEE Transactions on Mobile Computing, 2006.
[4] Nguyen, D. T, "Ad-Hoc Network Security Approaches", La Trobe University Library. (2008).
[5] Merwe, J., D. Dawoud, and S. McDonald, "A survey on peer-to-peer key management for mobile ad hoc networks". ACM Computing Surveys (CSUR), 2007.
[6] Capkun, S., L. Buttyan, and J. Hubaux, "Self-organized public-key management for mobile ad hoc networks". IEEE Transactions on Mobile Computing, 2003.
[7] Toh, C., "Ad Hoc Wireless Networks: Protocols and Systems". 2001: Prentice Hall PTR Upper Saddle River, NJ, USA.
[8] Haas, Z., "Wireless ad hoc networks. Encyclopaedia of Telecommunications", 2002.
[9] Akyildiz, I., "A survey on sensor networks". IEEE communications magazine, 2002.
[10] Morris, R,"CarNet: A scalable ad hoc wireless network system". 2000: ACM.
[11] Yang, H.,"Security in mobile ad hoc networks:challenges and solutions".IEEE Wireless Communications,2004.
[12] Cheng, X., X. Huang, and D. Du, "Ad hoc wireless Networking".2004: Kluwer Academic Pub.
[13] Belding-Royer, E., "Hierarchical routing in ad hoc mobile Networks". Wireless Communications and Mobile Computing, 2002.
[14] Boukerche, A., "Performance evaluation of routing protocols for ad hoc wireless networks". Mobile Networks and Applications, 2004.

Author Profile

Miss Aakanksha Jain received BE in Computer science degree from Truba Institute of Engg And Information Technology Bhopal, presently studying in NRI Institute Of Information Science & Technology Bhopal to complete M-tech degree in information technology stream.