IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. VIII (Nov – Dec. 2014), PP 44-47
www.iosrjournals.org

Detection and Prevention of Wormhole Attack in MANET Using DSR Protocol

Aashima[1], Vishal Kumar Arora[2]
[1]M Tech Student, [2]Assistant Professor
Deptt. Of CSE, SBSSTC, FEROZEPUR, 152001, PUNJAB, INDIA

Abstract: *With the advancement in wireless technologies, wireless networks are developing at a fast rate and so are the MANET's. Several routing attacks are introduced in the wireless networks due to their dynamically changing network topologies. A severe type of attack known as wormhole attack is the main theme of this paper and the work has been done to detect and prevent this attack. The work has been done with the help of DSR protocol. The existing functionality of DSR is extended so that the wormhole nodes are easily detected in the routing path and then that path is not used in the future because it is blacklisted by the network. A brief overview of the algorithm is also mentioned in the paper by which the detection and elimination of wormhole node is actually done.*

Keywords: *MANET; DSR; wormhole; detection*

I. Introduction

As MANET is a self configuring network with dynamic topology in which nodes have the property to easily deploy them in the network and change their position accordingly. In MANET, each one of the node acts as a host as well as router at the same time. Due to the lack of centralized management in MANETs, numereous routing attacks are suspected to be introduced in the network at any time.Security is a difficuilt case to handle in case of wireless networks as the mobile nodes can easily change their position and their topology is random. Different types of attacks are present in the network. The attacks can be categorized as active and passive attacks. In active attacks, the attackers not only listen to the data that is being transmitted but also they tamper the tamper the data. But in case of passive attacks, the attackers only listen the data being transmitted and use that information in a variety of ways. A severe kind of attack in MANET is wormhole attack whose detection and prevention is the topic of discussuion in this work. A description of the work done so farregarding wormhole attack detection and prevention has been mentioned in this paper and their solutions are also mentioned.[12]

The remainder of this paper is organized as follows. Section II contains introduction of the wormhole attack. Section **III** explains about DSR protocol. Section IV contains a short explanation of our proposed algorithm, the implementation of which is the target of our future work. Finally Section V concludes the whole paper.

II. Wormhole Attack

In wormhole attack, the two wormhole nodes are placed in between the center of the network and that strategic location is used to create a route from source to destination. The wormhole nodes have a interesting characteristic that they possess a shorter and faster path, so that the entire communication to be forced to go through them. If a link have these two properties then that path is surely used for communication. When wormhole nodes are introduced in the network, they try to validate its neighbouring nodes that they are its legitimate neighbours and the route through these nodes also exist.[1]

In the figure 1, it is shown that when source and sink want to communicate, S-A-B-C-D route is followed which is a normal route. When wormhole nodes X and Y are introduced into the network, they lure their neighbours S and D that they are their immediate neighbours and have a path between X and Y. The path between X and Y is a faster channel and compared to the other normal route this path is shorter in respect of hop counts and also X-Y path is faster. So the communication is forced to go through S-X-Y-D route. The wormhole nodes listen the data and they do whatever they want to do with the data.

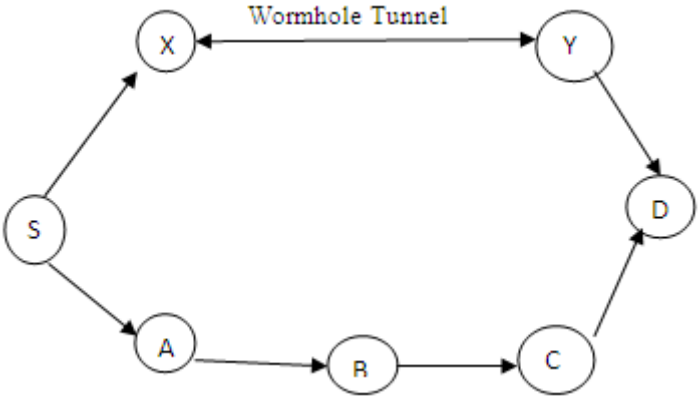

Figure 1: Wormhole Attack

S: Source
D: Destination
X,Y: Wormhole nodes
A,B,C: Normal nodes

III. DSR(Dynamic Source Routing) Protocol

A routing protocol is defined as the set of rules that are used to communicate and control the transmission between source and destination. MANET have three kinds of routing protocols:

a) Reactive Protocols – These are also known as on demand routing protocols. In this the communication is only done when source node wants to communicate with its sink. Eg. DSR
b) Proactive Protocols – These are also known as table driven protocols. In this each node maintains a routing table for different destinations. Eg. DSDV.
c) Hybrid Protocols – The routing protocols which have both proactive and reactive merits. Eg. EIGRP(Enhanced Interior Gateway Routing protocol).

DSR protocol is the topic of discussion in this section. In this protocol, a route is generated only when a source node wants a route to destination for communication to take place. Source node broadcasts the message to its neighbouring nodes to find a particular route from source to sink. The neighbouring nodes again forward the Route Request message to its further neighbour nodes so that a complete route is set up. When destination accepts that message, then it replies to the source via that path.[13][20]

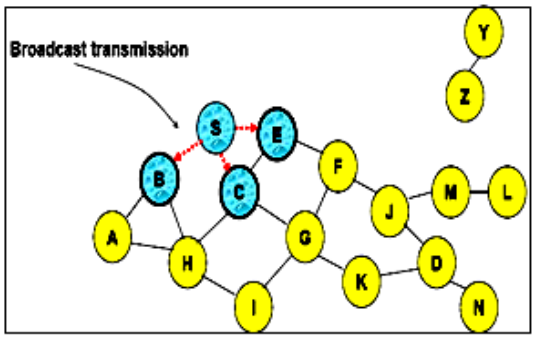

Figure 2: Route Request message to neighbours

In figure 2, node S broadcasts the route request message to its neighbouring nodes which further sends to their neighbours also. In this way, the destination node receive the meassage at last. Whosoever is the intended receiver, receives that message and destination replies to source node via that path from where the message came.

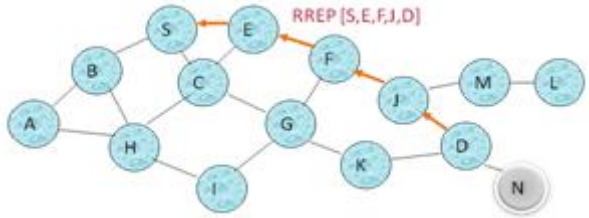

Figure 3: Route setup between Source and Sink

In the figure 3, Source node S sends the route request message to destination via S-E-F-J-D. When D receives that message, it replies via same path i.e. D-J-F-E-S. So this is how the DSR works.

IV. Proposed Work

Looking at the above discussions about wormhole attack and DSR protocol, it is clear that the route for communication is selected on the shorter length of the route i.e. route having less number of hop counts and moreover, wormhole nodes make a smaller as well as faster channel in between them. So the entire communication is done through them because of its properties like shorter and faster path between them.

We will explain our proposed solution by stating an example of figure 1 in which source and destination have to communicate. When X and Y are introduced they see that the hop count for route SXYD is 2 hop counts and hop cpunt for SABCD is 4. So the SXYD route is preffered because it is short. This is the main technique used while detecting.

When S wants to communicate with D, it initiates a route discovery phase with the help of DSR. DSR has the characteristic that it can only find a single route from S to D. Here the DSR functionality is extended. Multipath algorithm is applied at initial stage so that multiple paths are found from S toD. All those paths are stored in the routing table. When a route is found, hop count, delay and timer for a route also is stored in the routing table. From the routing table, when 1st route is selected for transmission, if in case its hop count is abruptly decreased in comparison to other route's hop count, then that path is isolated and a security mechanism is applied on that path.[2]

In our work, we assume that the wormhole nodes are already present in the network. If only a hop count for a route is comparitively less than only that path is isolated. Further the complete explanation of the algorithm is defined which is as such:

A. A Brief Overview Of The Algorithm

As stated above, wormhole nodes are identified only when the average hop count of a link is abruptly decreased in comparison to other paths because wormhole nodes possess a smaller hop count.

1) Step 1:

When source node wants to communicate with sink, a process starts to find multiple routes for communication to take place between two nodes.

2) Step 2:

When multiple routes are to be found from source to destination, hop count for a route is also saved in the routing table along with the delay and timer parameter.

3) Step 3:

From the saved rotes in the routing table, 1st route is selected and if that route's hop count is abruptly decreased as compared to other routes, then that route is isolated. And if that route has normal hop count then communication is done through that route.

4) Step 4:

On that Smaller hop count route, an encrypted message is send in which every legitimate node of the network adds its own key that is predefined in the network and is only known to valid nodes and if all the nodes on that route add a key, then that route is considered as a normal route with all the normal nodes. But if on that route, any node doesnot add the key, then that node is considered as a wormhole node and the route containing wormhole links is isolated from the network.

5) Step 5:

When a misbehaving node is found in the network, then the route containing that node is eliminated from the network and blacklisted also so that in future no such communication occurs through that route.

6) Step 6:

Wormhole nodes are detected in the network by the technique of hop count and then sending a security mesaage with key embedding. But without eliminating the wormhole node from the network, the attack is not prevented. Before elimination of wormhole node, the wormhole node is detected but not prevented. By the elimination of wormhole node and forged path, the wormhole attack is prevented.

V. Conclusion

Wormhole Attack is a serious kind of attack introduced in the network at the network layer of OSI Model. A number of work has been done to detect the wormhole attack but none of them proves so much valuable. Our work focuses on detection of the wormhole node by using hop count mechanism and applying security to the route having smaller hop count. When a route is detected with wormhole node then that path is removed from the routing table and this is the criteria for wormhole node detection and prevention of wormhole attack in MANET.

The future work includes the implementation of the algorithm using ns-2 simulator and the comparison of this work with some of the work present in the literature survey.

Acknowledgement

This work is supported by Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, INDIA and is currently under process.

References

[1]. Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak, "Wormhole Attack Avoidance Technique In Mobile Adhoc networks" Third International Conference on Advance Computing & Communication Technologies, IEEE 2013.
[2]. Rajpal Singh Khainwar, Mr. Anurag Jain, Mr. Jagdish Prasad Tyagi, "Elimination of Wormhole Attacker node in MANETs using performance evaluation multipath algorithm", International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 2,PP 40-47, December, 2011.
[3]. Weichao Wang, Bharat Bhargava, Yi Lu, Xiaoxin Wu, "Defending against Wormhole Attacks in Mobile Ad Hoc Networks", Conference of Wiley Journal Wireless Communications and Mobile Computing (WCMC), 2010 .
[4]. Shalini Jain, Dr.Satbir Jain, " Detection and prevention of wormhole attack in mobile adhoc networks", International Journal of Computer Theory and Engineering, Vol. 2, No. 1, pp 123-127, February, 2010.
[5]. Dr. Karim Konate, Abdourahime Gaye, "A Proposal Mechanism Against the Attacks: Cooperative Blackhole, Blackmail, Overflow and Selfish in Routing Protocol of Mobile Ad Hoc Network", International Journal of Future Generation Communication and Networking Vol. 4, No. 2, pp 156-158, June, 2011.
[6]. Shaik Madhar Saheb A. K. Bhattacharjee, A. Vallavaraj and R. Kar, "A Cross-Layer based Multipath routing protocol for IEEE 802.11E wlan", IEEE, pp-5-8, GCC conference and exhibition, February, dubai 2011.
[7]. Ms. N.S.Raote, Mr.K.N.Hande, "Approaches towards Mitigating Wormhole Attack in Wireless Ad-hoc Network", International Journal Of Advanced Engineering Sciences And Technologies Volume- 2, Issue- 2, pp 172 – 175, 2010.
[8]. L. Lazos, R. Poovendran, C. Meadows, P. Syverson, L. W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach", Research supported by NSF grand and Collaborative Technology Alliance.
[9]. Radu Stoleru, Haijie Wu, Harsha Chenji, "Secure neighbor discovery and wormhole localization in mobile ad hoc networks", SciVerse Science Direct, volume- 10, issue- 7, pp 1179-1190, 2012.
[10]. Farid Naït-Abdesselam, Brahim Bensaou, Tarik Taleb," Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks", Communications Magazine, IEEE, Volume- 46, issue- 4, pp 127-133, 2008.
[11]. Amol A. Bhosle, Tushar P. Thosar and SnehalMehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANETs", International Journal of Computer Science, Engineering and Applications (IJCSEA) Volume- 2,issue- 1, pp 325-331, February 2012.
[12]. L. Lazos, R. Poovendran, C. Meadows, P. Syverson, L. W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach", Research supported by NSF grand and Collaborative Technology Alliance.
[13]. Routing protocols and concepts, CCNA exploration companion guide. ''Introduction to dynamic routing protocols''. Chapter three pages 148 to 177.
[14]. http://www.ietf.org/rfc/rfc2501.txt , date last viewed: 2012-10-11.
[15]. Sung-Hee Lee, Young-Bae Ko, Youg-Geun Hong, and Hyoung-Jun Kim, ''A New MIMC Routing Protocol Compatible with IEEE 802.11s based WLAN Mesh Networks'', pp-126-131, ICOIN, International conference, IEEE, 2011.
[16]. Turgay Korkmaz ," Verifying Physical Presence of Neighbors against Replay-based Attacks in Wireless Ad Hoc Networks", Information Technology: Coding and Computing, ITCC, IEEE International Conference, volume- 2, pp 704-709, 2005.
[17]. Gajendra Singh Chandel, Priyanka Mur, "MANETs Threat Alarming Based On System Statistics & Support Vector Machine", International Journal of Engineering Research and Applications (IJERA), Volume- 2, Issue- 4, pp 1722-1726, July-August 2012. http://isi.edu/nsnam/ns/tutorial
[18]. Matthias Transier, "NS2 tutorial running simulations".
[19]. The Handbook of Adhoc Wireless Networks, By Mohammad Ilyas, Florida Atlantic University, Florida.