IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 12, December 2016

Detection of Vampire Attack in Wireless Adhoc Network

Kalyani S Kumar

Asst Professor, Department of ISE, GSSSIETW, Mysuru

Abstract: Mobile ad-hoc network is an infrastructure-less network in which the routing operation play important role in route discovery between communicating nodes. Due to infrastructure-less characteristic of ad-hoc network, it has different issues like routing, MAC layer, security etc. One of them is security issue which needs more concern. Vampire attacks modify targeted packets. It does so by preparing long routes or misguiding the packets. Malicious nodes use false messaging, or modify routing information. This action affects the bandwidth and node battery power. Routing as well as network resources gets protection from vampire attack; an approach is proposed to detect malicious routing packets. Present work gives result for different routing based attacks and discusses the issue of a serious resources consumption attack (Vampire Attack). The proposed approach uses the packet monitoring technique to detect malicious packet in the network. Proposed approach considers different network scenarios when using simulation. The basic principle behind the approach is that nodes check the received route request by comparing the packet header's information (broadcast id and destination address) during route discovery phase and discard the malicious packets. A comparative performance study is performed in requisites of packet delivery ratio, throughput, routing overhead and energy consumption. It is found that Network performance improves as compared to the existing approaches.

Keywords: Security, Algorithm, Wireless ad-hoc network, Routing, Security Issue, Vampire Attack.

I. INTRODUCTION

Wireless mobile ad-hoc network is a set of many nodes or terminal by means of wireless communication and network capability that communicate with each other with decentralized administrator [1]. These networks are basically a kind of wireless communication networks with mobility. Therefore, in such network major issues are found that is security and performance. A variety of routing algorithm exists and every routing strategy is efficient in one way or another depends upon the range of the network [2].

The prime objective of routing protocol in wireless network is to produce a path between sender and receiver by means of minimum number of route request packets and more bandwidth available to use [3]. Proposed work investigates the wireless ad-hoc networks for their security and performance issues. Due to observation these issues are basically dependent on the routing strategy by which the network nodes find routes for deliver the data. Most of the attackers take advantage of routing techniques because these techniques are easily able to deploy the attacks in such kind of networks. Several routing based attacks exist. More work is required for the vampire attacks in wireless ad-hoc networks. Proposed work focus on security therefore, different kinds of security issues are investigated.

II. RELATED STUDY

Eugene Y. Vasserman et al [4] discovered that every studied protocol are vulnerable to vampire attacks that are complex to discover and simple to introduce with the help of one malicious node transferring protocol-compliant messages. At its worst case, only single attacker is able to enlarge extensive battery power consumption by a factor of O (N), where N is number of nodes in network. Author discusses solution to moderate all vampire attacks that include a fresh proof-of-concept which provably limits the harm caused by attacker in duration of the packet forwarding phase.

P. Rajipriyadharshini et al [5] described a solution for vampire attack and described as wireless sensor network is a communication network across the sensor nodes. Sensor nodes collect information about use a physical environment. Now-a-days one main issue in wireless ad-hoc network is wastage of energy at each sensor device. New protocol called PLGP, a valuable and secure protocol is proposed along with the key management protocol called Elliptic Diffie-Hellman Key exchange protocol to avoid vampire attack.

P.Preeti Monolin [6] discussed about the wireless Adhoc networks and collected self-directed devices that are self-manage with infrasture-less characteristic. Because of their dynamic network formation, wireless ad-hoc network are susceptible to DDoS attacks-an illustration of a resource exhaustion attack, with energy as the resource of interest. That type of attack is known as “Vampire” attacks. Vampire attack is encounter in two phases: Topology Discovery and Packet forwarding phase where a cache reliability scheme is proposed.

DOI 10.17148/IJARCCE.2016.51219

Susan Sharon George [7] focused on a more devastating, complex to prevent, and simple to detect attack called vampire attack, which quickly drain nodes' battery power leading to the permanent disabling of nodes. Majority of the traditional routing protocols fail to provide security in this scenario. This paper introduces a novel protocol to mitigate these kinds of attack that limits the effect of vampire attack.

Fenye Bao [8] suggested a greatly scalable cluster based hierarchical trust management protocol for wireless sensor network to effectively compress to malicious nodes. On the basis of trust-based intrusion detection, they determine that there exist an optimal trust threshold for minimize fake positives as well as fake negatives.

Umakant et al [9] discussed about how routing approaches influence through wrong activity. This research proposed EWMA methods to blind the harm because of resource consumption type attack during packet forwarding phase.

Yuanming Wu et al [10] considered frequent security vulnerabilities that are watchdog and trust mechanism and observed how inside attacks exploit these defense holes and finally recommend defending approaches that can moderate the weakness of trust technique and watchdog.

Jose Anand et al [11] proposed a method to detect the presence of vampire attack and the simulation result show the energy consumption in each case.

III.PROPOSED METHODOLOGY

The detailed methodology is described for implementing the proposed approach for detecting vampire attack. Basically vampire attack is a variant of DDOS attack, which performs resource consumption on neighbor nodes. Therefore, targeted packets are modified for preparing long routes or misguiding the packets during the vampire attack.

The malicious nodes are making frequent connectivity from the entire neighbor nodes in network using false control message exchange. Due to this neighbor nodes reply to false request for connectivity and draining energy rapidly. Therefore, in order to identify the malicious packets in network a new kind of scheme is required which monitor the network nodes' activity and provide the decision for malicious packet.

The malicious node just changes the received packet's information during vampire attack. For simulation purpose when a malicious host receives route request packets then it changes the destination address to an unreachable or unknown host IP address. This result all packets are continuous flooded in the network. Once the false packets are flooded by the hosts it can increases the network bandwidth consumption.

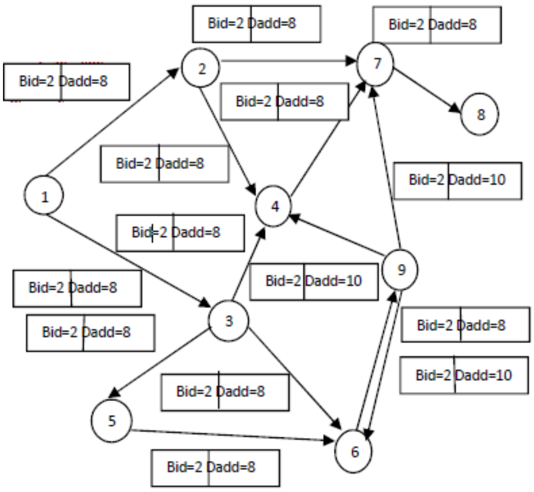

FIG 1: SCENARIO FOR VAMPIRE ATTACK DETECTION

Fig 1 shows steps in vampire attack detection. Number of nodes and route request with broadcast id and destination address are given. Node 1 is a source node, node 8 is a destination node and node 9 is a malicious node that modifies the received packet's information. Node 1 initiates route discovery process and send RREQ packet to their neighbor nodes with broadcast id 2 and destination address 9. This RREQ packet processed by their neighbor nodes. When node 9 receives that RREQ packet then modify the destination address and append the address of unknown host. Modified packet continuously flooded in the network. In order to overcome the effect of malicious packets, compare all received RREQ in every node. For comparison, extract broadcast id and destination address oh all RREQ packets and compare them. If broadcast id and destination address are same then forward the packet otherwise discard the packet.

IV. ALGORITHM

This section describes algorithm of proposed approach. The nodes can check intermediate host and can discard the malicious packet during route discovery phase. Therefore, proposed work performs check on the received packets information before forwarding to other host. Broadcast id of received packet along with the destination address of received packet is checked in this algorithm

```
Step1: Initialize with Number of Received RREQ Packets

Step2: IF (Received_RREQ_Packet ==1) THEN
Forward the RREQ packets
ELSE IF (Received_RREQ_Packet ==2) THEN
Ignore RREQ and wait for new one
ELSE IF (Received_RREQ_Packet < RREQ limit) THEN
REPEAT i =1 to Received_RREQR_Packet -1
Extract bid [i] , dadd [i]
IF (bid [i] == bid [i+1] && dadd [i] == dadd [i+1]) THEN
```

```
Flag=1
ELSE
Flag=0

Step3: IF (Flag ==1) THEN
Forward the RREQ packet
ELSE
DISPLAY (“Malicious RREQ Packet”)
Step4: Exit
```

V. CONCLUSION AND FUTURE WORK

The key objective of the proposed work is to discover an optimum solution for vampire attack in wireless ad-hoc networks. Therefore, an approach is developed for securing the network. The experimentation and experiment outcomes give essential facts for proposed approach. Comparative performance study is performed with respect to the existing approach in order to justify the proposed approach’s effectiveness. It is concluded that performance of the proposed approach is adaptable due to high bandwidth availability, low energy consumption, higher packet delivery ratio and less routing overhead.

Proposed approach is an efficient and effective approach and able to detect the malicious packet in the wireless network. But the performance of proposed approach is decreases as the number of nodes increases frequently. But for the small network and small number of nodes the performance of network is much adaptable. Therefore, in near future the proposed approach is improved for supporting more number of efficiently.

REFERENCES

[1] S. Buruhanudeen, "Existing MANET routing protocol and metrics used toward the efficiency and reliability-An Overview," IEEE Telecommunication and Malaysia International Conference on communication, pp. 231-236, 2007.

[2] T. W. Mehran Abolhasan, "A review of routing protocols for mobile ad hoc network," ELSEVIER, Ad-hoc Network, vol. 2, pp. 1-22, 2004.

[3] M. B. Hardeep Kaur, "Performance of AODV, OLSR AND ZRP Routing Protocol under the black hole Attack in MANET," IJAREEIE, vol. 2, pp. 2320-3765, June 2013.

[4] N. H. Eugene Y. Vasserman, "Vampire Attack: Draining Life from Wireless Ad-hoc Sensor Networks," IEEE Transaction on mobile computing, vol. 12, no. 2, pp. 1-15, February 2013.

[5] V. V. P. Rajipriyadharshini, "Vampire Attacks Deploying Resources in Wireless Sensor Network," International Journal of Computer Science and Information Technology, vol. 5, no. 3, pp. 2951-2953, 2014.

[6] D. J. A. P. Preethi Monoline, "Cache Consistency and IDS for Handling Attacks in Routing Ad-hoc Network," International journal of Innovative Research in Computer and Communication Engineering, vol. 2, no. 4, 2007.

[7] S. R. Susan Sharon George, "Attack-Resistant Routing for Wireless A- hoc Network," Internattional Journal of Computer Science and Information Technologies, vol. 5, no. 3, pp. 420- 442, 2014.

[8] I.-R. C. Fenye Bao, "Hierarchical Trust Management for Wireless Sensor Networks and its Application to Trust-Based Routing and Intrusion Detection," IEEE Transaction on network and service managemnet, vol. 9, no. 2, July 2012.

[9] J. D. B. Umakanth, "Detection of Energy draining attack using EWMA in Wireless Ad-hoc Sensor Network," International Journal of Engineering trends and Technology, vol. 4, no. 8, August 2013.

[10] Y. Yuanming Wu, "Insider Threats against Trust Mechanism with Watchdog and Defending Aproaches in Wireless Sensor Networks," IEEE Symposium on Security and Privacy workshop, 2012.

[11] K. S. Jose Anand, "Vampire Attack Detection in Wireless Sensor Network," International Journal of Engineering Science and Innovative Technology, vol. 3, no. 4, July 2014.