ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

A Survey of Malicious Packet Dropping Attacks in Wireless Ad Hoc Networks

G.Vanithamani[1], K.Mythili[2]

M.Phil Scholar, Hindusthan College of Arts and Science, Coimbatore, India. [1]

Associate Professor, Hindusthan College of Arts and Science, Coimbatore, India. [2]

ABSTRACT: This survey paper describes two sources of packet losses in multi-hop wireless ad-hoc network. Link error and malicious packet dropping are important sources of packet losses in wireless network. We determine the causes of link error and malicious drop. In the case of insider-attack, malicious nodes are exploiting their context to selectively drop the packets At the moment network performance is critical, because in the case of packet dropping rate is comparable to the channel error rate, conventional algorithms are based on detecting packet loss rate is not accuracy. This paper discusses various methodologies of path deduction and packet drop.

KEYWORDS: Packet dropping, secure routing, attack detection, Wireless Ad-Hoc network

I. INTRODUCTION

The wireless ad-hoc network is a self-organized network without using any pre-Existing infra-structure. The nodes are directly communicate to each other, But intermediate nodes are connected to the Neighbour nodes. Wireless ad-hoc network is sending information from source to destination. At the time of network will select the path in a particular way. In case of path selection in a linear way, any one node can drop the packet it can't reach the destination. At the moment of network information not reach the end node. So completely disturbs all the nodes for source to destination. The security issues related to wireless ad hoc network is unstructured, because the topology changes make it unstructured. It provide low quality communication due to open nature, environmental factors are affect the wireless network. This paper describes various protocols are used malicious packet dropping attacks in wireless ad hoc networks.

II. OVERVIEW OF PROTOCOLS

Here, we are using three kinds of protocols for,

A. AODV protocol
B. DSR protocol
C. OLSR protocol

A. AODV PROTOCOL

The ad-hoc on demand distance vector routing protocol is a routing protocol for Mobile ad hoc network and wireless ad hoc network.[4] AODV obtain quick destination for mobile nodes. In case of link breakages, timely change the network topology. It allows the mobile node and establish the route Quickly.[1]protocol work in two phases:1)route discovery process 2)Route maintenance process. The route recovery process work in Route request (RREQs)[11] and Route reply messages (RREPs), (RRERs) Route errors, and the route request (RREQs) finds the optimal path. If a node is the destination or a valid route to the destination give the reply message (RREPs) back to theSource. (RERRs) messages are used to notify the network of a link breakage. [12]Nodes communicate with each other without the intervention of base stations. In such a network, each node acts both as a router and as a host.
The limited transmission range of wireless network interfaces; multiple hops are needed to exchange data between nodes in the network.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

B. DSR PROTOCOL

The Dynamic source routing protocol (DSR) is simple and efficient protocol designed to use Wireless ad-hoc network for mobile nodes. It composed by two mechanisms that work together to allow route discovery and route maintenance in the ad-hoc network. [2]In a communication in the network, nodes send ROUTE REQUEST message to all the nodes. All nodes having this message to update the routing table. This route is forwarded to their neighbour nodes. If a receiving node is the destination, or a route to the destination act as an intermediate node, it does not forward the request it sends a REPLY message containing the full source route. In case of a link failure due to poor network signal, packets cannot forwarded one node to another node and send the error messages to the source node.

C. OLSR PROTOCOL

Optimized link state routing (OLSR) is a proactive protocol it contains higher overhead then other proactive protocols. In which routing information is given by every node to another node, OLSR used efficient forwarding mechanism called multipoint relaying (MPR).It employs an optimized flooding mechanism for link state information. The topological changes cause the flooding information to available hosts in the network. [3]Multipoint relay design is used to less flooding during every route packets. The main functionality of OLSR using three different messages. Hello, TC (Topology Control) and Multiple Interface Declaration (MID).

Hello: All neighbour nodes are transmitted information by Hello messages. These messages are used for finding the information about link state routing and MPR calculation.

TC (Topology Control): Topological Control messages are the condition signal done by OLSR. These messages are propagate all over the network, calculate the routing information and also update periodically

MID (Multiple Interface Declaration): The Multiple interface declaration messages are forwarded by nodes running OLSR for more than one interface. These messages are circulated the entire network using by MPR.

III.**RELATED WORK**

S.Amutha,K.Balasubramanian, explained the paper "**Secure Implementation of Routing Protocols for Wireless Ad hoc Networks**" [5],Routing is a fundamental networking function in every communication system also wireless Ad hoc networks. On ad hoc network routing protocols disrupt the attacks for network performance and reliability. The intermediate nodes are corrupted and exhibit arbitrary behaviour. The pair of secret keys given the protection in route discovery messages for source to destination. The performance of the existing routing protocols compared with Dynamic Source Routing (DSR) and Ad hoc On-demand Distance Vector (AODV).It is difficult to keep addresses on each nodes.

Heni KAANICHE1, Fatma LOUATI2, Mounir FRIKHA3 and Farouk KAMOUN1 discussed the paper "**A Qos routing protocol based on available bandwidth Estimation for wireless ad hoc network**" [6] AODV, by the reactive nature, a bandwidth is less important for the service of the tables of routing than the proactive protocols. In fact, these last generate massive control traffic between useful periods of communication while the reactivity of AODV reduces the load of network in term of messages control since path towards destinations are established only at the request of the sources of traffic data.

David B. Johnson David A. Maltz Josh Broch explained the paper" **DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks**"[7]The Dynamic Source Routing protocol (DSR) provides excellent performance for routing in multi-hop wireless ad hoc networks. DSR has very low routing overhead and is able to correctly deliver almost all originated data packets, even with continuous, rapid motion of all nodes in the network completely self-organizing and self-configuring network among themselves. Our current work in the Monarch Project at Carnegie Mellon University includes further improvements to the performance of DSR the most efficient use of the best available network connections at any time.

Bounpadidth, Hidehisa Nakayama, Nei Kato, Yoshiaki Nemoto and Abbas Jamalipour [8] *described the paper* "**Analysis of Node Isolation Attack against OLSR based mobile ad hoc networks**". By using OLSR protocol information regarding neighbour node is obtained by broadcasting the hello message. This hello message performs the task of sensing the neighbour nodes and MPR selection process.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

A nodes hello message contains its own address, a list of its 1-hop neighbour's and a list of its MPR set. Therefore by exchanging hello messages, each node is able to obtain the information about its 1-hop neighbour and can find out which node has chosen it as an MPR. In order MPR must generate a topology control (TC) message periodically. A nodes TC message contains a list of MPR selector set. Upon receiving TC message of all MPR nodes in the network.
Each node learns all nodes MPR set and hence obtains the knowledge of the whole network topology. Based on this topology, the nodes are able to calculate routing table. Each entry in the table consists of destination address, next hop address, distance and nodes own address. The routing table's calculation is based on Dijkstra's algorithm for finding shortest path.
The routing table is updated when a change is detected in 1-hop neighbour and 2-hop neighbour. It is recalculated in case of neighbour lost or 2-hop neighbour is created or removed. They have proposed a model called node isolation attack model where victim node is detected and isolated from the network by hearing hello message and TC message periodically. The victim node can only forward the fake hello message but it is unable to generate and forward TC message. The drawback is that it might not detect the attack which is launched by two consecutive nodes who work in collusion.

*Rajendra V. BoppanaAnketMathurdescribed the paper ''***Analysis of the Dynamic Source Routing Protocol for Ad Hoc Networks**" DSR[9] is a widely used routing protocol for mobile ad hoc networks, but has very low delivery rates and poor performance in lightly loaded networks with high node mobility. Several of the modifications proposed in the literature such as turning off intermediate node replies improves the performance somewhat. Improve the performance of DSR.
Factorial analysis indicates that both limited replies and one route per destination improve performance significantly and the third feature does not impact performance. While multiple routes may benefit at higher traffic loads, keeping only one route per destination helps sender nodes gather routes when the topology changes. Without using any complicated strategies, our proposed techniques perform significantly better than previously proposed modifications at very low traffic loads (50-100 Kbps) and about the same at higher traffic loads.

DeniLumbantoruan1,AlbertSagala2 discussed the paper" **Performanceevaluation of OLSR routing protocol in ad hoc network**" [10]Based on testing result includes testing the availability of ad hoc networks with 3 and 4 hops, testing ad hoc network coverage, OLSR routing by using Raspberry Pi devices as nodes can be implemented. Through several testing scenarios can be seen that the ad hoc network built can be used to overcome the limitations within range, by implementing of multi hop communication.
By doing testing with scenarios such as range testing, multi-hop testing, and wireless ad hoc network self-healing can be concluded that the Raspberry Pi by using USB Wireless TP-Link WN722N with OLSR routing protocol can work well with distances up to ± 180 meters between two nodes in one hop in line of sight communication. When the number of hops increase then it will decrease delivery ratio and increase the delay, but the system can still work well. Through testing we can also find that the self-healing mechanism performed successfully. Testing by using video access applications on the server shows that even though the intermediate node switch to another node, users can still access the video server properly.

IV. COMPARISON OF VARIOUS PROTOCOLS IN PACKET DROP ATTACKS

	AUTHOR	TITTLE	PROTOCOL	ADVANTAGES	DIS ADVANTAGES
1.	S.Amutha,K.Balasubramanian	Secure Implementation of Routing Protocols for Wireless Adhoc Networks	AODV,DSR	secret keys given the protection in source to destination	It is difficult to keep addresses on each nodes
2.	Heni KAANICHE1, Fatma LOUATI2, Mounir FRIKHA3	"A Qos routing protocol based on	AODV	AODV reduces the load of	control establish sources of traffic of data only

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

	and Farouk KAMOUN1“	available bandwidth Estimation for wireless ad hoc network		network	
3.	David B. Johnson David A. Maltz Josh Broch	DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks	DSR	Data packets are delivered correctly	very low routing overhead
4.	Bounpadidth, Hidehisa Nakayama, Nei Kato, Yoshiaki Nemoto and Abbas Jamalipour	“Analysis of Node Isolation Attack against OLSR based mobile ad-hoc networks	OLSR	High Throughput	Not detects the attacks in collusions
5.	Rajendra V. BoppanaAnketMathur	” Analysis of the Dynamic Source Routing Protocol for Ad Hoc Networks	DSR	benefit at higher traffic loads	
6.	Deni Lumbantoruan1 , Albert Sagala2	Performance evaluationof OLSR routing protocol in adhoc network	OLSR	Self-healing mechanism performed successfully.	

V. CONCLUSION AND FUTURE WORK

In this survey paper discuss the above protocols and its methods. These protocols are used and deduct the packet drop attacks. Various authors using the various protocols such as dynamic source routing (DSR), Ad-hoc on-demand distancevector(AODV),optimizedlinkstate routing(OLSR).These methods are provide some advantages but not Reliable. Some of the disadvantages are occur the collusion and difficult to keep the address on the nodes. In future effective methods can be developed and overcome the disadvantages.

REFERENCES

1. David B. Jhonson ,DavidA.Maltz and Josh Broch „ DSR: The Dynamic Secure Routing protocol for Multi-Hop WirelessAdhocNetworks.http://www.monarch.cs.cmu.edu.
2. MurizahKassimRuhaniAbRahman, Mariamah Ismail Cik Ku HaroswatiChe Ku Yahaya,” Performance Analysis of Routing Protocol in WiMAX Network,” IEEE International Conference on System Engineering and Technology (ICSET), 2011
3. M.Gunasekar ,S.J.Hinduja , “ Tuning of OLSR routing protocol using IWD in VANET”, International Journal of Innovative Research in Computer, Volume 2, Issue 1, March 2014.
4. Dr.C.KumarCharliepaul 1 K.Megala Devi2” secure routing and attack deduction in wireless ad hoc network” International Journal On Engineering Technology and Sciences , IJETS, Volume I, Issue VI, OCT – 2014.
5. S.Amutha,K.Balasubramanian,”Secure Implementation of Routing Protocols for Wireless Adhoc Networks” Australian Journal of Basic and Applied Sciences, 9(5) March 2015.
6. Heni KAANICHE1 , Fatma LOUATI2 , Mounir FRIKHA3 and Farouk KAMOUN1 “A QOS routing protocol based on available bandwidth estimation for wireless ad hoc networks” international journal of computer networks &communications, volume 2,2011
7. David B. Johnson David A. Maltz Josh Broch” DSR: The Dynamic Source Routing Protocol for Multi-Hop
8. Wireless Ad Hoc Networks” International Journal On Engineering Technology and Sciences ,January 2002.
9. Bounpadidth, Hidehisa Nakayama, Nei Kato, Yoshiaki Nemoto and Abbas Jamalipour [11] described a paper titled “Analysis of Node Isolation Attack against OLSR based mobile adhoc networks” in computer Networks,2006 International Symposium.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

10. Rajendra V. BoppanaAnketMathur" Analysis of the Dynamic Source Routing Protocol for Ad Hoc Networks" International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 4, April 2014.
11. DeniLumbantoruan1,AlbertSagala2"Performanceevaluation of OLSR routing protocol in adhoc network" International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.2, No.2, June 2011.
12. Ali Khosrozadeh1 ,Abolfazle Akbari2 , Maryam Bagheri 3 and Neda Beikmahdavi4" A New Algorithm AODV Routing Protocol in Mobile ADHOC Networks" Int. J Latest Trends Computing, Vol-2 No 3 September, 2011.
13. Harmandeep Singh, Gurpreet Singh, Manpreet Singh" Performance Evaluation of Mobile Ad Hoc Network Routing Protocols under Black Hole Attack" International Journal of Computer Applications (0975 – 8887) Volume 42– No.18, March 2012.