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 9, September 2016

Self Adaptive Routing Framework with Faux Node Generation to Detect and Mitigate OLSR Security Threats

Shyam Chandran P[1], Anupama K N[2]

Assistant Professor, Department of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu[1]

Research Scholar, Department of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu[2]

Abstract: Wireless networks are infrastructure less. Due to this nature, many types of security threats affect Ad-hoc network process and performance. In this proposal, different types of attacks and its mitigation strategy over ad-hoc network are discussed and finally proposed a new routing framework for OLSR to detect and defend DOS and wormhole attacks. In the infrastructure free network, the abnormal and malicious behavior of nodes disturbs the overall performance of the network, so the detection should be accurate and should reduce packet delay and loss. In existing, various techniques and methods used to mitigate different types of attacks and security threats in OLSR protocol. The proposed system concentrates on the DOS and Wormhole attack issue in OLSR. So the proposed system designs and implements a new routing framework named as **SAR (Self adaptive routing framework with faux node generation)**, which detects and mitigates the routing attacks in OLSR. The self adaptive framework provides effective mitigation process on dynamic node isolation and wormhole behaviors.

Keywords: MANET, OLSR, node isolation attack, faux node.

I. INTRODUCTION

A Mobile Ad-Hoc network [MANET] consists of many mobile nodes and have free infrastructure. In this type of network the nodes are unbound to join up with the network at any moment. This unbound nature cause's lot of security checks and energy related issues in the network. Mobile node in MANET has limited transmission range and every node act as a router as well to forward packet [1]. In MANET, mitigation of such attacks may cause some routing issues and energy consumption problems so several techniques and protocols are introduced and implemented. Such protocols are categorized into two types one is proactive routing protocols and reactive protocols. In this paper, we are handling the proactive protocol OLSR (Optimized Link State Routing) with security considerations. Even though OLSR is quite effective in bandwidth utilization and in path computation, OLSR is defenseless to various attacks such as DOS (Denial of Service) attack and several routing attacks. These types of attacks arise due to the random, dynamic, rapidly changing topology and limited bandwidth of nodes [2].

The followings are the attacks possible in a Mobile Ad hoc network [3]. Some of them are:

A. NODE ISOLATOIN ATTACK:

1. Node isolation attack

Node isolation attack is a kind of Denial of Service (DOS) attack whose goal is to isolate a node from communicating with other nodes within the network. Node isolation attacks allows attacker to drop victim nodes and other set of nodes route information by dropping TC (Topology Control) message. Consequently, other nodes could not able to receive route information of the victim node. Hence those nodes become not available and isolated from network.

2. Black Hole attack:

The attacker who is active on a compromised node advertises that the node has the shortest route to the destination node in whose packets he is interested in. Then all the nodes of the network would adjust their routing table accordingly and route all the packets to the particular node through the compromised node only, which may drop or alter the packets. It's also a kind of DoS attack.

3. Worm Hole attack:

This attack has two adversaries who are connected through a private line which is not a part of the network. The packets received by one of the attacker are sent to the other attacker through the private line and the other attacker rebroadcast the packets, thereby utilizing the network resources and spreading fake information about routes in the network.

4. Partition attack:

The adversary makes false route advertisements in such way that the network is divided into different sets, which either not reachable at all or reachable only through the attacker.

DOI 10.17148/IJARCCE.2016.59109

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 9, September 2016

5. Rushing attack:
In this the RREQs are processed/forwarded without considering the MAC (Medium Access Control) layer and routing protocol specifications, thereby increasing its chance to be selected as an intermediate node in the route. In this paper we will mainly concentrate on wormhole attack identification.

6. Malign attack:
In this attack malicious nodes blackmails a good node and spoils its reputation.

7. Resource Consumption Attack:
In this the intruder tries to consume the node's resources such as battery power, computational resources, such as bandwidth, disk space, processor time by sending the forged RREQ packets to the nodes.

8. Detour attack:
In this the adversary publicizes the routes such that the nodes are made to take detour routes to reach their destination or may not reach the destination at all.

9. Route Invasion Attack:
In this the intruder sends fictitious RREQ packets and tries to add itself to the route through which the source and destination of its interest are communicating.

10. Jelly Fish attack:
This attack has following features a) delivery all packets in scrambled order b) selective black hole c) holding received packet for a longer time.

B. OLSR Overview:
OLSR protocol optimizes a pure link state protocol for MANETs by reducing the size of control packets (CP), which does not transmit the packet to all links. Instead of declaring all links, it declares only a subset of links with its neighbors. And it reduces flooding and controls traffic by using only selected nodes, which is also known MPR (Multi Point Relays). In OSLR Only the MPR node retransmits its broadcast messages [4].

OLSR protocol has the following process,

- **Every Node in MANET sends topology information in Topology Control (TC) messages. The TC message contains the following details [5].**

  - List of advertised neighbors (link information)
  - Sequence number (to prevent use of stale information)

- **A node generates TC messages only for those neighbors in its MS(Multipoint Relay set selector)**

  - Only MPR nodes generate TC messages
  - Not all links are advertised.

- **A nodes processes all received TC messages, but only forwards TC messages if the sender is in its MS set [6]**

  - Only MPR nodes propagate TC messages

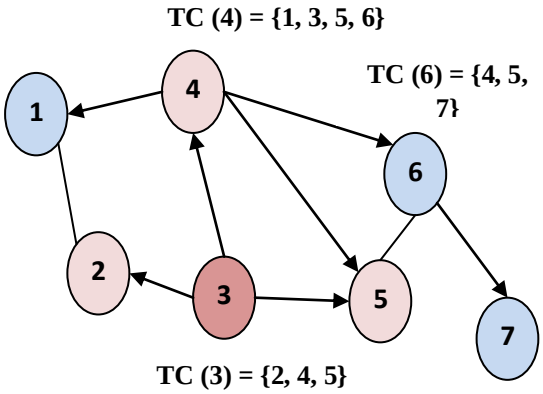

Fig 1.0 OLSR example

In Fig.1.0 Node 3 have three MPRs which are 2, 4 and 5. This protocol is basically suitable for dense networks. The protocol does not belongs to any central authority, and it works completely in a distributed manner. In OLSR, Hop by hop routing is performed.

In OLSR, every node generates a TC (Topology Control) message by Giving TC information, each node forms a topology table based on the link. And the routing table is calculated from the topology table.

From the fig 1.0, Node 3 generates a TC message to the advertising nodes in MS(3) = {2, 4, 5} and Node 4 forwards Node 3's TC message since Node 3 ∈ MS(4) = {1, 3, 5, 6} and Node 6 forwards TC(3) since Node 4 ∈ MS(6) .Node 6 generates a TC message advertising nodes in MS(6) = {4, 5, 7}, Node 4 forwards TC(6) from Node 6 and Node 3 forwards TC(6) from Node 4 ,After Nodes 3, 4, and 6 have generated TC messages, all nodes have link-state information to route to any node.

II. RELATED WORK

In [7] [8], the authors make use of public key infrastructure (PKI) algorithm to perform secure routing. It makes use of additional details, which contains information about time stamp and signature of every node. Every node maintains a table where the information is gathered in header message and it is stored for verifying the correctness of the link state information. This technique imposes a large overhead to the network in terms of additional traffic and signature computation which result in high energy consumption at each node.

This technique also improves security in a MANET running on OLSR routing protocol using a fully distributed Certificate Authority. It improves the control traffic load compared to using a centralized Certificate Authority. Still malicious nodes with proper credentials could not be identified. In [9] the authors employed distributed key management techniques in order to defend against wormhole and message replay attacks in MANET. In [10], depicted security threats to the OLSR MANET routing protocol. A semantic based intrusion detection solution was unfilled. The semantics properties are based on semantic properties implied in the OLSR routing

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 9, September 2016

behavior. But several existing solution did not address conflicts resolution and verification procedure for intruders.

In [11] authors reduced the cost of service in the network by make use of authentication system based on one-way hash chain. The cost of the password is used to ensure the authentication, when comparing this parameter the proposed system is much less than DVSIG.
In [12] the authors propose one more way to authenticate, MPR selected Node by sending 2-hostrequest to 2-hop node. If node replays with the 2-hostreplay packet then MPR selected is authenticated MPR. But there is one overhead is added after MPR selection.

Momentous amount of work has been done regarding the security of ad hoc networks and honey pot but a few on the combination of both. Some of them have given new protocols while the others have given methods to secure already existing ones. In [13] the authors calculate the minimum number of hops to reach the destination by measuring its geographical location using GPS whereas in paper [14] use the average RTT(Round Trip Time) to identify the attack and then compare the neighbor list of the fake neighbors in process to detect it. Paper [15] provides an in-depth understanding of way the attackers behave by observing their interactions with a high interaction honey pot. In [16] the authors have elucidated the different kinds of honey pot approach to implement them and also the legal issues and challenges to be taken into consideration when a honey pot is implemented. In [8] the author has identified a honey pot based method to find the black hole attack in infrastructure based Wireless Mesh Network using virtual honey pots.

III. PROPOSED SYSTEM

Wireless network utilize the node mobility and opportunistic contact among nodes for data communication, because the network structure is infrastructure less. Due to this nature, many types of security threats affect Ad-hoc network process and performance. In this paper, we focused on different types of attacks and its mitigation strategy over ad-hoc network. In the infrastructure free network, the abnormal and suspicious behavior of nodes affects the overall performance of the network. In this thesis, we surveyed various techniques and methods used to mitigate different types of attacks and security threats in OLSR protocol. In this paper overview of OLSR, features of OLSR along with the attack detection and mitigation techniques comparisons are made. Finally a new approach against wormhole and DOS attack is proposed.The proposed system focuses on the DOS and Wormhole attack issue in OLSR. So the proposed system designed a new routing framework named as SAR (Self adaptive routing framework with faux node generation), which detects and mitigates the routing attacks in OLSR for high security. The self adaptive framework provides effective mitigation process on dynamic node isolation and wormhole behaviours.

A. SAR (Self Adaptive Routing Framework With Faux Node Generation)

SAR mechanism is introduced to improve the security of the OLSR routing protocol against two different types of attacks. In this solution, each node receives an authentication key and signs in its HELLO and TC messages. These signatures are later used by others to prove their own HELLO and TC messages. This authentication process prevents nodes from declaring Fake Faux nodes without sufficient activity score. SAR provides a number of techniques to identify abnormal behavior on the network. The solution includes a message sent in response to the detection of an attack, allowing for the exclusion of compromised nodes and preventing them from being included in network routing tables. The SAR framework has the following techniques.

- Time stamp calculation technique
- ETR-Expected Transmission Rate calculation
- Network Coding Techniques

1. System Initial Setup Procedure:

The step by step description of the proposed SAR scheme is as follows:

Node initialization with node parameters is initiated in the first step. In this 50 wireless nodes are created. In the first step, SAR registers all the valid mobile nodes and also generates private key for all the register nodes.

- When a mobile node A registers with the SAR, it keeps the record of mobile nodes by storing the identity of mobile node with the node activation time-stamp (Ts).
- To provide the additional security against various attacks the SAR sends registration information encrypted with the hash function H like (Hash (SAR), Ts).
- After receiving the broadcasted information from the SAR, all the sensor nodes present in the network will reply by sending their acknowledgements respectively.
- In addition, if a mobile node will not receive any information, it won't send any ACK to the server.

2. After node initialization, for every nodes **Time stamp calculation process (Ts)** will begin

This helps to detect the exact activate time of every node in the network. This **t**ime stamping is the process of securely keeping track of the creation and modification time of a node and its mobility. Security here means that no one not even the node can be able to change it once it has been recorded provided that the timestamper's integrity is never compromised.

The creation of node timings can be back dated. A timestamp is a 64-bit, signed fixed-point number in seconds and fraction with the decimal point to the left of bit 32. Dated stamps are used in internal calculations where extended range and freedom from overflow are important, while timestamps are used in packet headers where economy of storage is important. The system clock interface (SCI) is the only source of time used by the SAR for times stamp calculation process. It provides two data

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 9, September 2016

types, timeval (gettimeofday ()) and timespec (get clock()). Both data types represent the time in seconds past 0h, 1 January 1970. In timeval format the second is represented in microseconds, while in timespec format the second is represented in nanoseconds. In either format, the Unix time must be converted to an SAR data type before use.

3. Authentication Process:

After successful registration of a mobile node, authentication process will be performed by the receiving nodes. In this SAR, authentication is very important process as it provides strong defense against the above specified attacks. Once the authentication procedure is successful, both sending and receiving mobile nodes will generate their MPR activation key. The generation of the MPR activation key will be performed. The steps of the initiated authentication process are described in the following steps.

Step1: Initially the mobile node S sends a communication request to Mobile node R. To initiate secure communication, these have encrypted the communication message with the private key of the sending mobile node. It also includes timestamp Ts in the encrypted message.

Step2: After receiving communication request, receiving node R will verify the identity of the sending mobile node S and its MPR list.

a. After the verification, before mobile node R sends the reply message, it will calculate the time difference (ΔT) between Tc (Current timestamp) and Ts (Activating time stamp). This sets a threshold on the time difference, if it is less than 20 milli-seconds than mobile node R will send its identity along with its timestamp and signature else go to the Step 1 again.

Step3: After the authentication process, mobile node R will reply by sending reply message which includes that MPR list and Ts.

Step4: mobile node S will perform the same steps as Step2 and verify the registration of mobile node R and again calculate the time-difference (ΔT) between Tc (Current timestamp) and Ts (Sending time stamp).

4. ETR-Expected Transmission Rate calculation

ETR is defined as the expected number of MAC layer transmissions that is needed for successfully delivering a packet through a wireless link. The weight of a path is defined as the summation of the ETR of all links along the path Energy consumption for a data transmission only depends on

$$k - 1(1 - p) = \frac{1}{1 - p}$$

$$kp \quad ETR = \sum_{k=1}^{n}$$

Here, k means that the transmission times for node S send a packet to node R successfully. And p means error rate of the transmission. Since both long paths and lossy paths have large weights under ETR, the ETR metric captures the effects of both packet loss ratios and path length. In addition, ETR is also an isotonic routing metric, which guarantees easy calculation of minimum weight paths and loop-free routing under all routing protocols. However, energy consumption of the devices is not taken into consideration in ETR. So it is done separately.

(1) The size of the data packet
(2) The distance between the sender and receiver

Residual Energy (E) = (Total energy-(totalpkts * avgenergy_of_each_packet))

5. Network Coding Techniques

The network coding techniques is nothing but , appending the Ts in every packet header and the index of MPR list. From the above technique, the system creates a FAUX node for successful data transmission. At the same time FAUX node creation by the vulnerable node will be limited by a set of predefined rules.

IV. RESULTS AND ANALYSIS

A. Simulation Configuration

The simulation is carried out within the Network Simulator 2. in Linux operating system with Ubuntu as the interface tool. The mobility model uses the random waypoint model. There are 50 nodes defined in a simulation area of size 1000m x1200m. The mobility of nodes is limited to 7ms. The traffic model chosen is Constant Bit Rate (CBR) connections with packet size of 1024 bytes to emulate traffic over the network.

B. Performance results:

The performance of our proposed work SAR using FAUX node scheme is compared with the existing approach DCFM. This considered the MPR selection on the OLSR at the time of verification.

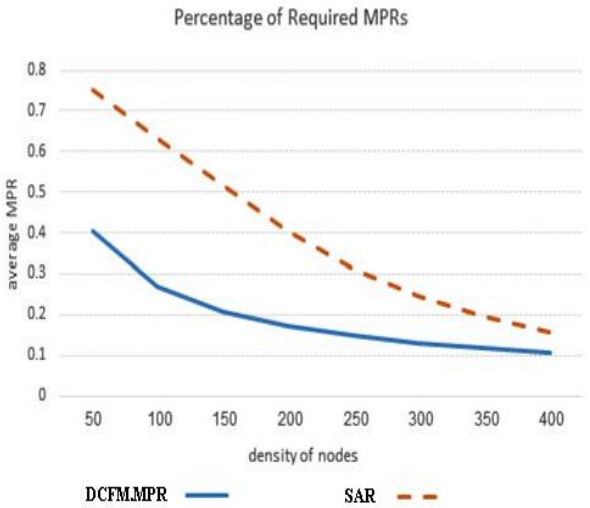

Fig 2.0 Number of required MPRs, depending on the network density

Fig. 2.0 presents the overhead costs as the number of nodes in the network increases. The X axis represents the number of nodes in a random network topology, while the Y axis represents the percentage of nodes, again, as a function of nodes in the network that were selected as MPRs. The SAR compared with the existing DCFM method in the form of MPR list. The DCFM system only provides less MPR when the total number of nodes is increased. SAR provides very high MPR when compared with the existing system.

V. CONCLUSION

In this paper, a new framework for OLSR is proposed, that is named as SAR .It uses different algorithms and techniques to defend and detect the DOS, wormhole attacks and locate the attacker in MANET. For a dynamic network like MANET, SAR efficiently provides security against those attacks. With the help of activity score and other minor historical information's SAR effectively finds the attacker. The major advantage of the system is that, if a new node is compromised, the attacker can be immediately detected and isolated from the network. With the use of FAUX node creation, the transaction will be successfully made. Using SAR, It limits the false alarm and improves transaction efficiency in OLSR.

REFERENCES

[1] S. Mclaughlin, D. Laurenson, and Y. Tan, "Mobile ad-hoc network." (Aug. 10 2006) uS Patent App. 11/351,777. [Online]. Available: http://www.google.com/patents/US20060176829
[2] T. Clausen and P. Jacquet, "IETF RFC3626: Optimized link state routing protocol (OLSR)," Experimental, 2003
[3] T. Clausen and U.Herberg, "Security issues in the optimized link state routing protocol version 2 (OLSRv2)," Int. J. Netw. Security Appl.,2010.
[4] Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "Securing the OLSR protocol," in Proc. Med-Hoc-Net, 2003.
[5] Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "An advanced signature system for OLSR," in Proc. ACM SASN, 2004.
[6] Dhillon,D.,Randhawa,T.S., Wang,M. and Lamont,L. "Implementing a Fully Distributed Certificate Authority in an OLSR MANET," IEEE WCNC2004, Atlanta, Georgia USA, March 21-25, 2004
[7] Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "Attacks against OLSR: Distributed key management for security," in Proc. OLSR Interop and Workshop, 2005.
[8] Tseng, Chinyang Henry, et al. "A specification-based intrusion detection model for OLSR." International Workshop on Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2005.
[9] Adjih, Cédric, et al. "Securing the OLSR routing protocol with or without compromised nodes in the network." HIPERCoM Project, INRIA Rocquencourt, Tech. Rep. INRIA RR-5494 (2005).
[10] Hiba Sanadikia, Hadi Otrokb, Azzam Mourada, and Jean-Marc Robert "Detecting Attacks in QoS-OLSR Protocol" IWCMC, 2013.
[11] Khadidja Ayad, Thouraya Bouabana-Tebibel,"New efficient mechanisms to secure OLSR protocol" FGCT 2012.
[12] Nguyen, Dang, and Pascale Minet. "Analysis of MPR Selection in the OLSR Protocol." Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on. Vol. 2. IEEE, 2007.
[13] Mauve, Martin, Jorg Widmer, and Hannes Hartenstein. "A survey on position-based routing in mobile ad hoc networks." IEEE network 15.6 (2001): 30-39.
[14] Esposito, Pedro Miguel, et al. "Implementing the expected transmission time metric for OLSR wireless mesh networks." 2008 1st IFIP Wireless Days. IEEE, 2008.
[15] Prathapani, Anoosha, Lakshmi Santhanam, and Dharma P. Agrawal. "Intelligent honeypot agent for blackhole attack detection in wireless mesh networks." 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems. IEEE, 2009.
[16] Prathapani, Anoosha, Lakshmi Santhanam, and Dharma P. Agrawal. "Detection of blackhole attack in a Wireless Mesh Network using intelligent honeypot agents." The Journal of Supercomputing 64.3 (2013): 777-804.