ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Review Article*
www.ijptonline.com

A SURVEY ON TRUST-OLSR ROUTING BASED SECURE TRANSMISSION IN MOBILE AD-HOC NETWORKS

[1]V. Nancy, [2]T.Balachander
[1]PG Student, CSE Department, SRM University, Kattankulathur.
[2]Assistant Professor, CSE Department, SRM University, Kattankulathur.
Email:nanzy.jesi@gmail.com

Received on 07-01-2017 *Accepted on: 15-02-2017*

Abstract

Ad hoc networks have the trust factor present among their entities in routing operations. As wireless networks work on limited nodes, it is important for the nodes to cooperate and communicate with the neighbouring nodes to extend the network with the remote nodes. In this paper we involve in the trust factor as a solution for OLSR protocol. This approach is suitable for Adhoc networks. The trust factor among the entities makes them to reason out and take decisions depending on the entities. In this research we propose a prototype called the Trust- OLSR (TOLSR) which is based on cooperation and routing operation and attacker detection and prevention. The technique and its contribution and explained in detail in trust-based security in OLSR. A trust based analysis is held for OLSR protocol using trust specification language and we demonstrate how trust based reasoning enables to evaluate the behaviour of the other nodes. Using this method we will detect the misbehaving nodes and then we propose solutions to prevent and counter measure the problem and resolve the situation of inconsistency. We also offer cryptography based security algorithm.

Keywords: MANET, OLSR, TOLSR, ECC.

Introduction

MANET- Mobile Adhoc Network is a self organized communication mode with mobile nodes and without a central coordinator. The node in the MANET can be any mobile device that has the ability to communicate with other nodes. The nodes in the MANET network work as both as a host and as a router. The unique feature of MANET over traditional methods is its ease to be set up and destroyed and also the flexible nature of the nodes. Optimized Link State Routing (OLSR) protocol is a commonly used algorithm today. OLSR is efficient in using the bandwidth and in path calculation but it is vulnerable to attacks. Since this prototype is dependable on the cooperation between network

nodes it is easy to confuse rogue nodes and at times even a single malicious node can destroy the entire network set up. The possible attacks on OLSR are flooding attacks, spoofing attacks, black-hole attacks, colluding mis-relay attacks and DOS attacks. In this paper we involve in the trust factor as a solution for OLSR protocol. This approach is suitable for Adhoc networks. The trust factor among the entities makes them to reason out and take decisions depending on the entities. In this research we propose a prototype called the Trust- OLSR (TOLSR) which is based on cooperation and routing operation and attacker detection and prevention. The technique and its contribution and explained in detail in trust-based security in OLSR. A trust based analysis is held for OLSR protocol using trust specification language and we demonstrate how trust based reasoning enables to evaluate the behaviour of the other nodes. Using this method we will detect the misbehaving nodes and then we propose solutions to prevent and counter measure the problem and resolve the situation of inconsistency. We also offer cryptography based security algorithms like ECC security algorithm. ECC delivers tremendous speed and efficiency and many researchers say that it is never been defeated. We improve the existing encryption and decryption techniques and deliver excellent security.

MANET

With a lot of portable devices around us it is important to have a speed and secured wireless communication. For this purpose we need to implement ad-hoc networking to a widespread of applications. Ad-hoc as the name terms it all that this network can be set up anywhere with little or no communication infrastructure. Ad-hoc networks are so scalable that adding and removing a device from the network is easily done without altering the network performance. MANET is applied to several applications which ranges from mobile, large-scale, static networks and small networks. Apart from the traditional applications moving or migrating to the Ad-hoc environment there are a whole set of new services that are supported by MANET. Some of the typical applicants include Military Batttlefield: Since most of the equipments used in military contain some sort of computer device, ad-hoc helps to path the network between soldiers, military headquarters and vehicles. PAN- Personal Area Network: MANET helps in establishing a short range network that includes PCs, laptop, and mobile devices. MANET-VoVoN: This is a MANET enabled version of JXTA. It is used to support user location and audio streaming over the JXTA network.

Existing

Since most of the applications and networks are tending towards ad-hoc topology and specifically in MANET network, it is more prone to attacks and vulnerability. Hence improving the security of this prototype is highly in demand. There are several solutions being proposed for various types of attacks but these solutions lead to network

overload and affect the efficiency of the network. To specify, the major attack on the OLSR is the node isolation attack which happens when the topological knowledge of the network is exploited by an attacker where the affected node is isolated from the network and hence communication services are denied to the victim. This paper talks on a novel solution for the above problem to defend the OLSR protocol from node isolation attack. The simulation results demonstrate that the proposed method prevents more than 95% of attacks.

Backpressure Algorithm

Backpressure routing is the concept of dynamically routing the traffic in a multi-hop network using congestion gradients. This algorithm can be applied to wireless networks that include mobile ad-hoc networks (MANET), heterogeneous networks, and sensor networks. The concept of backpressure is applicable in the study of product assembly systems and processing networks. This method mainly focuses on the communication of the network, where packets from multiple data streams arrive and has to be delivering to the concerned destinations. This methodology works on the principle of slotted time. The time slot helps in routing the data in the direction where the differential backlog is maximal between the neighbouring nodes. This is very similar to the concept of water flowing through pipes through pressure gradients.

Hence the backpressure algorithm is applicable to various network topologies where different packets have different destinations and also in networks where transmission rates can be selected. Notable features of this algorithm are i) maximum network throughput ii) robust iii) it is not dependable on the traffic arrival rate or channel state probability. However there are some drawback in backpressure where it is difficult t be implemented. It is vastly being studied theoretically.

Wormhole

As we know that MANET is made up of mobile nodes that move independently in an open environment. Communication can happen between these mobile nodes through intermediate routers. Some qualities of MANET like the open medium, lack of centralized monitoring, lack of clear defence system and dynamic network topology makes it vulnerable for various attacks. There is a high possibility that the intermediate nodes can be malicious and cause threat to the network. Wormhole is a common attack in case of ad-hoc networks. One malicious node transports the packets to another malicious node. So if in case the source node decide to choose the path which contains these malicious nodes then the packets can either be delivered or eavesdropping can happen. In the case of sample22.tcl, the wormhole attack establishes a transmission between nodes using the UDP agent and CBR traffic.

Sinkhole

Sinkhole is another attack for the MANET topology. In this attack the malicious node sends fake routing information to other nodes stating that it is the optimum route to achieve the target. Hence the malicious node will be able to reach the target without any traffic and tamper the data. In this paper we show the implementation of Sinkhole on MANET with DSR routing protocol using Netsim.

Blackhole

As stated earlier in MANET there is high possibility that the intermediate nodes can be hampered through attacks and threats. Blackhole is one such attack in ad-hoc networks where the malicious node acts a routing node and states itself as the shortest path to achieve the target or destination. Once it is being considered as the optimal path, it receives all the data packets and drops the data packets instead of routing them forward. In the case of sample22.tcl, the wormhole attack establishes a transmission between nodes using the UDP agent and CBR traffic. The source node does not send the data to the destination and the attackers do not forward the data to the neighbours.

Optimized Link State Routing (OLSR)

The Optimized Link State Routing (OLSR) is a routing protocol based on table and exclusively developed for MANETs. It helps in reducing the size of the control packet and also the number of control packets transmission required. OLSR uses the MPR- Multipoint relays to control traffic. MPR is a node's one-hop neighbour that is chosen to forward the packets. Instead of just pure flooding the network the packets are just forwarded in MANET by a node's MPRs. Hence it delimits the network overhead.

OLSR works best in a large and dense network environment. Hence the more dense and larger the network the more optimized the link state routing is framed.

MPRs provide the shortest path to the destination and the requirement to do so is that all MPRs declare the link information for their MPR selectors.

Control messages

In OLSR there are three kind of messages used: Topology Information (TC), Multiple Interface Declaration (MID) and HELLO. Hello message is used to be sent periodically to all of the node's neighbours. The hello message contains information about the nodes that are selected as MPRs and to the list of neighbours whose bidirectional links are not confirmed. The below figure shows the format used for “Hello” message.

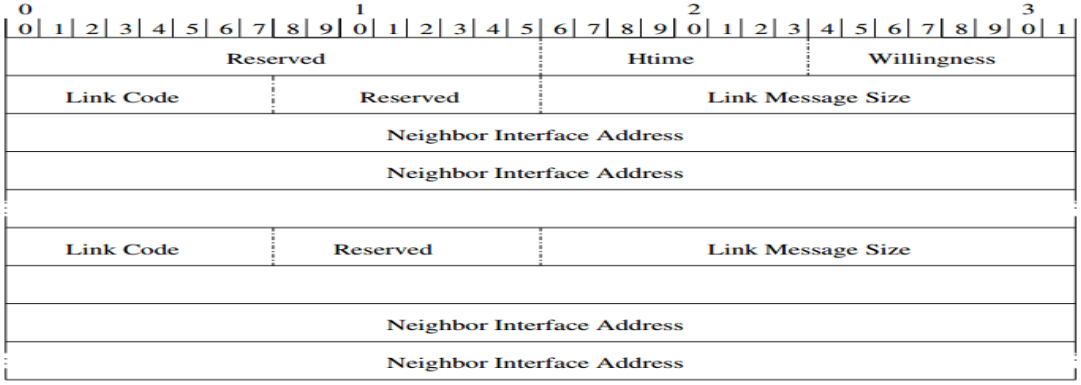

Figure 1.1. Format of OLSR HELLO packet.

All the nodes periodically floods using the multipoint relying mechanism, the network with a TC message. This message will contain the node's MPR Selector set.

MID message is used to broadcast that a node is running OLSR in more than one interface. This message is flooded to the entire network by the MPRs.

Elliptic Curve Digital Signature Algorithm Signing

For signing a message m by sender A, using A’s private key d

1. Calculate e = HASH (m), where HASH is a cryptographic hash function, such as SHA-1

2. Select a random integer k from [1,n − 1]

3. Calculate r = x1 (mod n), where (x1, y1) = k * G. If r = 0, go to step 2

4. Calculate s = k − 1(e + dr)(mod n). If s = 0, go to step 2

5. The signature is the pair (r, s)

Elliptic Curve Digital Signature Algorithm Verification

For B to authenticate A's signature, B must have A’s public key Q

1. Verify that r and s are integers in [1,n − 1]. If not, the signature is invalid

2. Calculate e = HASH (m)

3. Calculate w = s −1 (mod n)

4. Calculate u1 = ew (mod n) & u2 = rw (mod n)

5. Calculate (x1, y1) = u1*G + u2*Q 6. The signature is valid if x1 = r(mod n)

TOLSR protocol: overview

TOLSR uses optimized flooding mechanism to send partial link state information to all network nodes. It is a proactive link-state routing protocol. TOLSR uses multi-point relays (MPR) where selected nodes forward the

broadcast messages during the process of flooding. This link state information will be generated only by those that are selected as MPRs. The selected MPRs should only broadcast the state of links between the selector and itself. There are two messages used in this topology namely: HELLO and TC- Topological Control. These messages allow each node to obtain and declare network topology information. These two messages have validity time that indicates how long the information can be considered.

The functionality of TOLSR can be described in three steps: neighbourhood discovery, MPR selection and Routing table calculation. The trust relationship is also estimated between the TOLSR nodes. This trust analysis helps in identifying the trust assumption in different steps of the protocol and how it can be used by the attackers.

Related work

P. Jacquet et al [1] discusses on the optimized link state routing protocol called OLSR for mobile wireless networks. The algorithm is based on link state algorithm. It exchanges messages periodically to maintain topology information of the network at each node. OLSR is an optimization process over a pure link state protocol. It helps in optimizing the size of information sent in the message and also reduces the number of retransmissions of the broadcast data. For this the algorithm uses multipoint relaying technique to economically and efficiently manage flood its control messages. The proposed method is best suitable for dense and large ad-hoc networks.

Yih-Chun Hu et al [2] proposes the wormhole attack in MANET. This attack is the most severe attack in ad hoc networks and it can attack even if the attacker has not compromised any hosts and even if there is authenticity and confidentiality in all communications. In the wormhole attack the attacker records the packets at one location, tunnels them to another location and retransmits them there into the network. The wormhole attack can cause severe damage to ad-hoc networks and also in location-based wireless security systems.

M. Wang, L. Lamont et al [3] introduces threats to the OLSR MANET routing protocol and also proposes a solution based on protocol semantics checking. This approach is based on the semantic properties and specifies the correct OLSR routing update behaviour. When any abnormal protocol semantics are found it triggers an intrusion alarm. The OLSR can be applied on Multi-Point Relay (MPR) proactive MANET protocol.

D. Dhillon et al [4] proposes an algorithm with PKI implemented with OLSR MANET in the network layer level. The OLSR control packets are used in this method to support various security activities. A fully distributed CA (Certificate Authority) is used in this method and integrated with an existing implementation of OLSRv4 (OLSR for IP version 4).

Bounpadith Kannhavong,et al [5] experiments a new routing attack called the Node Isolation attack against the Optimized Link State Routing (OLSR) protocol. The attack is studied in detail through experimental results to show the requirement to find counter measures to protect the network against the attack. A simple technique is proposed by the author as a first step to defence and identify the source of attack.

Danny Dhillon et al [6] implement the Intrusion Detection System (IDS) where each node in the MANET evaluates the non-conformances locally. After which the possible attacks are found in the routing protocol. The effectiveness of IDS is measured in terms of false positive and false negative detection rates. Though the concept is based on OLSR it can be implemented on any link-state routing protocol.

Daniele Raffo et al [7] framed the paper to improve the security of OLSR routig protocol against several attackers. In specific the author targets on the mechanism used for message sending and sender authentication is deployed in this novel method. The author proposes a solution based on the recording recent routing information that is the HELLO message and reusing this information to prove the link state of a node. This is achieved through a new ADVSIG control message. The mathematical evaluation comprises of a maximum 192 + 288n additional bits for each HELLO sent and 192+160n additional bits for each TC sent. Though it is an expensive approach the advantage of using is it offers the advantage of securing the network against some major attacks coming from the nodes. The author has also identified further weaknesses in the new system and simulations are also estimated to extend the research.

Conclusion and Future Enhancement

We proposed a network called the TOLSR in which hop-by-hop or end-to-end will provide reliability. The main objective of this research is to explore the various ways of encryption. Utilise the existing methods and improvise them with few aspects to create reliability and strong security. These various features can be implemented on different large scale networks to study the security offered. Encryption is done using the AES-Advanced Encryption standard and ECC- Elliptic Curve Cryptography.

References

1. P.Jacquet, P.Muhlethaler, T.Clausen, A. Laouiti, A. Qayyum, L.Viennot, “Optimized Link State Routing Protocol for Ad Hoc Networks”, 0-7803-7406-1/01/$17.00©2001 IEEE.
2. Yih-Chun Hu, Adrian Perrig, and David B. Johnson, “Wormhole Attacks in Wireless Networks”, 0733-8716/$20.00 © 2006 IEEE

3. M. Wang, L. Lamont, P. Mason, M. Gorlatova, "An Effective Intrusion Detection Approach for OLSR MANET Protocol",0-7803-9427-5/05/$20.00© 2005 IEEE
4. D. Dhillon, T. S. Randhawa, M. Wang, L.Lamont,"Implementing a Fully Distributed Certificate Authority in an OLSR MANET", WCNC 2004 / IEEE Communications Society
5. Bounpadith Kannhavong, Hidehisa Nakayama, Abbas Jamalipour ," Analysis of the Node Isolation Attack Against OLSR-based Mobile Ad Hoc Networks", 1-4244-0491-6/06/$20.00©2006 IEEE
6. Danny Dhillon , Jerry Zhu, John Richards , Tejinder Randhawa ,"Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs", IWCMC'06, July 3–6, 2006, Vancouver, British Columbia, Canada. Copyright 2006 ACM 1-59593-306-9/06/0007...$5.00.
7. Daniele Raffo , C´edric Adjih "An Advanced Signature System for OLSR", SASN'04, October 25, 2004, Washington, DC, USA. Copyright 2004 ACM 1581139721/ 04/0010 ...$5.00.
8. P. Suresh, R. Kaur, M. Gaur, and V. Laxmi, "Collusion attack resistance through forced mpr switching in olsr," in Proc. Wireless Days, Oct. 2010, pp. 1–5.
9. A. Nadeem and M. Howarth, "Protection of manets from a range of attacks using an intrusion detection and prevention system," Telecommun. Syst., vol. 52, no. 4, pp. 2047–2058, 2013.
10. A. Nadeem and M. P. Howarth, (2014). An intrusion detection & adaptive response mechanism for manets. Ad Hoc Netw. [Online]. vol. 13, pp. 368–380. Available: http://www.sciencedirect.com/ science/article/pii/S1570870513001959
11. A. Nadeem and M. Howarth, "A survey of manet intrusion detection & prevention approaches for network layer attacks," IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2027 2045, Oct.-Dec. 2013.
12. D. Raffo, "Security schemes for the olsr protocol for ad hoc networks," Ph.D. thesis, Universit_e Paris, 2005.
13. [Online]. Available: http://www.nsnam.org/, Oct. 2013.
14. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Commun., vol. 11, no. 1, pp. 38–47, Feb. 2004.
15. B. Kannhavong, H. Nakayama, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE trans. Wireless Commun.*, vol. 14, no. 5, pp. 85–91, Oct. 2007.
16. T. Clausen and P. Jacquet, "IETF RFC3626: Optimized link state routing protocol (OLSR)," *Experimental*, 2003.

17. T. Clausen and U.Herberg, "Security issues in the optimized link state routing protocol version 2 (OLSRv2)," *Int. J. Netw. Security Appl.*, 2010.
18. B. Kannhavong, H. Nakayama and A. Jamalipour, "A study of routing attack in OLSR-based mobile ad hoc networks," *Int. J. Commun. Syst.*, 2007.
19. B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Analysis of the node isolation attack against OLSR-based mobile ad hoc network," in *Proc. ISCN*, 2006, pp. 30 35.
20. D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "Securing the OLSR protocol," in *Proc. Med-Hoc-Net*, 2003.
21. D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "An advanced signature system for OLSR," in *Proc. ACM SASN*, 2004.
22. D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "Attacks against OLSR: Distributed key management for security," in *Proc. OLSR Interop and Workshop*, 2005.
23. C. Adjih, T. Clausen, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the OLSR routing protocol with or without compromised nodes in the network," HIPERCOM Project, INRIA Rocquencourt, Tech. Rep. INRIA RR-5494, Feb. 2005.

Corresponding Author:
Nancy V*,
Email: nanzy.jesi@gmail.com