International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 5, September- October 2017 ISSN 2278-6856

Optimized Link State Routing - A Review

JayashreeAgarkhed
Professor, Department of C.S.E, P.D.A College of Engineering,
Kalaburagi, India.

Abstract— ***The security provisioning for routing in Mobile ah-hoc Networks (MANET) is a significant challenge to address. Various protocols have focused to maximize network lifetime by managing topology information in efficient manner. An Optimized Link State Routing Protocol known as OLSR is presented in literature which is adaptive to the energy consumption resulting in longevity of lifetime of the network without compromising the performances like throughput, end-to-end delay or overhead. OLSR experiences less delay to find a route due to its proactive nature with the expense ofresources. This paper reviews research carried out on the extensions of the OLSR protocols to scale well with dense network as well to handle security threats as MANET is more vulnerable to various kinds of attacks.***

Keywords— OLSR, MANET, Security

I. INTRODUCTION

Routing in MANET can be broadly classified as reactive, proactive and hybrid protocols. In Reactive routing approach the routes are acquired and maintained on demand. Whereas in proactive approach all nodes maintains routes to all destinations in the network at all times. The OLSR belongs to the family of proactive protocols wherein periodic update messages are exchanged to update topological information at each node. That is, topological information is flood to all nodes in the network, providing routes immediately available with a constant, low control traffic overhead regardless of data load and node mobility causing link breakage.

OLSR comprises of three generic elements which are given as follows.

- A mechanism for neighbour sensing
- A mechanism for efficient flooding of control traffic,
- A specification to select and diffuse enough topological information in the network in order to provide optimal routes [1].

Advantages of OLSR routing protocol are as folllows

- The pro-activeness capability best suited for dynamic topological changes.
- Easy integration
- Multiple interfacing
- Protocol can be extended
- High density networks
- Short transmission delays

MANET should have finest routing mechanism in terms of data delivery and data integrity as finding the routing paths and selection of most suitable path are the two major aspects in designing of any wireless network. The protocol selectionprocedure involves the performance analysis of the protocols. There are many measures in evaluation of the protocols. Among them most commonly used parameters are mean delay, throughput, routing overhead and packet delivery ratio [2].

Rest of the paper is organized as follows. Section II deals with related work. Section III deals with optimized link state routing and its extensions. Section IV concludes the work.

II. RELATED WORK

Enormous literature survey has been done on routing protocols in wireless ad hoc network. The routing packet through the network is a challenging task. OLSR is an example of a proactive routing protocol for MANETs.
The optimization of pure link state routing is known as OLSR as small size of information is sent in the messages. In addition, it floods these messages economically by multipoint relaying technique to entire network which reduces the number of retransmission required. Optimal routes with minimum number of hops are determined as soon as they are needed. This protocol works best for large and dense ad hoc networks [3]. A Quality of Service (QoS) metric is encompassed into OLSR routing protocol in MANET, which found more appropriate metric than the hop distance. From the simulation study, the performance improvement of QoS extension of LOSR is justified when compared with best effort OLSR [4].

MANETs are autonomous, selfconfigured and adaptive and hence becomes potential candidates for military tactical networks which requires rapid functioning without any centralized administration. Multi-hop routing is preferred when radio range is limited usually in such scenarios.The emphasis of the measurements is on the performance of the network with the mobile nodes [5]. Authors in [6] have investigated the possible attacks in MANET and have proposed the counter methods to alleviate such attacks. The authentication check of information is injected into the network. Even with perfect authentication check, replay attacks are still possible. An authentication mechanism by distributing public keys in a MANET is provided. The authentication of the message is carried out by a mechanism proposed in [7] which consists of signing each OLSR control packet with a digital signature. Further the timestamp exchange process provided by the security mechanism is used to prevent replay attacks on the routing protocol. Synchronized time is not required by this mechanism. The security issues on OLSR have not yet

addressed in the Internet Engineering Task Force (IETF) draft proposals. A care should be taken to avoid additional control traffic load in OLSR as much as possible while providing security using the public key infrastructure which found more appropriate security means in MANET [8].

III. EXTENSIONS TO OLSR

MANETs are autonomous and decentralized wireless systems. Many reliable routing protocols have been proposed such as Ad-hoc On demand distance vector (AODV), Dynamic Source routing (DSR), Zone routing protocol (ZRP), Temorarly Ordered Routing Algorithm (TORA) and the OLSR protocol to improve the routing performance in presence of route breaks due to mobile nodes in MANET**.** The comparative analysis in [9] shows that the AODV, TORA performs well in dense networks than OLSR in terms of measured parameter such as packet delivery ratio. Further, the OLSR protocol is more vulnerable to various kinds of attacks as security aspects have not been devised into it. Following are the few of the extensions proposed in literature to the OLSR protocols.

i. Hierarchical OLSR

In OLSR, the control packets are flooded to almost all interfaces, loading the network heavily. Further OLSR is not able to recognize the differences between transmission capabilities of the nodes and channel access control schemes used by the nodes. during route computation which makes its unsuitability to heterogeneous networks. In order to limit the control traffic overhead and to make more efficient use of the higher capacity links strategies have found in heterogeneous wireless networks. A hierarchical scheme, an extension to OLSR is proposed in [10] which shows that the Hierarchical OLSR (HOLSR) greatly minimizes the protocol overhead, enhancing the protocol scalability in heterogeneous network of large size.

ii. Clustered OLSR

A Clustered OLSR (C-OLSR) is an extension proposed for OLSR protocol making scalable to large dense network. The advantageous feature of clustered network is that the network is partitioned into clusters and hence limiting the propagation of control messages within the cluster. The clustering feature overcomes the overhead due to the proactive nature of the traditional OLSR which floods nodes in the entire network. The performance improvisation of C-OLSR over OLSR is justified in terms of generated overhead and throughput [11].

iii Secure OLSR

The past works in MANET have mainly concentrated on developing efficient routing mechanisms focusing on the stringent characteristics of MANET such as highly dynamic due to mobile nodes and network with the limited resources. However, these networks are more vulnerable to various kinds of attacks in the presence of malicious nodes [12]. The main approach proposed in [13] is based on authentication checks of information injected into the network. However even with the perfect verification check, replay attacks are still possible. However, due to their inherent characteristics, they are much more vulnerable to malicious attacks than a conventional wired network. In MANET, routing plays an important role in providing connectivity for mobile nodes that are not within the same radio range. Existing routing protocols in MANET assume a trusted and reliable environment. In argumentative environment, mobile nodes are susceptible to various types of routing attacks. It is analyzed and demonstrated the impact of this attack in order to show the necessity for a countermeasure to guard against the attack [14].

Recently research developments have been taken place to incorporate security in OLSR by using authentication and encryption techniques against attacks from the intruders.A second line of defense is required to provide intrusion detection and response techniques in protecting the OLSR protocol against attacks from inside intruders. The security threats to the OLSR protocol in MANET are discussed. Further based on protocol semantics checking an intrusion detection solution is proposed in [15]. This approach specifies the correct OLSR routing update behavior and conflict checking is applied in every node based on semantic properties. An intrusion alarm is triggered if any abnormal protocol semantics is observed.

Rapid advances in wireless networking technologies have made it possible to construct a MANET which can be applied in infrastructure less situations. Because of their inherent characteristics, MANETs are vulnerable to various kinds of attacks which aim at disrupting their routing operations. To develop a strong security scheme to protect against these attacks it is necessary to understand the possible form of attacks that may be launched. In recent literature various possible attacks against MANET have been proposed and investigated. However, there are still unanticipated or sophisticated attacks that have not been well studied. Authors in [16] proposeda collusion attack model against OLSR protocol in MANET. The OLSR occasionally sends control packets to build and update the topology due to its proactive feature. An extension known Fast-OLSR is developed to meet the need for fast mobility in MANETs [17].

IV. CONCLUSION

The unique characteristics such as varying network topology due to the presence of mobile nodes, resource constraints in MANET has challenged the design of routing protocols a greater challenge. Many routing protocols have been propsed in MANET and broadly can be classified as proactive, reactive and hybrid routing protocols based on the nature of route computation. The OLSR being proactive minimizes connection setup delay at the expense of heavier control traffic load on the wireless

channel. And hence does not scale well to dense larger network. Extensions to OLSR have been proposed by dividing the network into clusters, adopting hierarchical routing improves the performance. Further MANET routing infrastructure is more vulnerable to various attacks. Security mechanisms are incorporated in OLSR to counter these attacks.

REFERENCES

[1] Clausen, Thomas, et al. "The optimized link state routing protocol, evaluation through experiments and simulation." IEEE Symposium on" Wireless Personal Mobile Communications. 2001.
[2] Adjih, Cedric, et al. "Securing the OLSR protocol." Proceedings of Med-Hoc-Net. 2003.
[3] Huhtonen, Aleksandr. "Comparing AODV and OLSR routing protocols." Telecommunications Software and Multimedia (2004): 1-9.
[4] Munaretto, Anelise, et al. "A link-state QoS routing protocol for ad hoc networks." Mobile and Wireless Communications Network, 2002. 4th International Workshop on. IEEE, 2002.
[5] Plesse, Thierry, et al. "OLSR performance measurement in a military mobile ad hoc network." Ad Hoc Networks 3.5 (2005): 575-588.
[6] Toutouh, Jamal, José García-Nieto, and Enrique Alba. "Intelligent OLSR routing protocol optimization for VANETs." IEEE transactions on vehicular technology 61.4 (2012): 1884-1894.
[7] Hafslund, Andreas, et al. "Secure Extension to the OLSR protocol." OLSR Interop and Workshop. Vol. 1004. 2004.
[8] Dhillon, Danny, et al. "Implementing a fully distributed certificate authority in an OLSR MANET." Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE. Vol. 2. IEEE, 2004.
[9] Kuppusamy, P., K. Thirunavukkarasu, and B. Kalaavathi. "A study and comparison of OLSR, AODV and TORA routing protocols in ad hoc networks." Electronics Computer Technology (ICECT), 2011 3rd International Conference on. Vol. 5. IEEE, 2011.
[10] Ge, Ying, Louise Lamont, and Luis Villasenor. "Hierarchical OLSR-a scalable proactive routing protocol for heterogeneous ad hoc networks." Wireless And Mobile Computing, Networking And Communications, 2005.(WiMob'2005), IEEE International Conference on. Vol. 3. IEEE, 2005.
[11] Ros, Francisco J., and Pedro M. Ruiz. "Cluster-based OLSR extensions to reduce control overhead in mobile ad hoc networks." Proceedings of the 2007 international conference on Wireless communications and mobile computing. ACM, 2007.
[12] Kannhavong, Bounpadith, et. al. "A survey of routing attacks in mobile ad hoc networks." IEEE Wireless communications 14.5 (2007).
[13] Adjih, Cedric, et al. "Securing the OLSR protocol." Proceedings of Med-Hoc-Net. 2003.
[14] Kannhavong, Bounpadith, et al. "Analysis of the node isolation attack against OLSR-based mobile ad hoc networks." Computer Networks, 2006 International Symposium on. IEEE, 2006.
[15] Wang, Maoyu, et al. "An effective intrusion detection approach for OLSR MANET protocol." Secure Network Protocols, 2005.(NPSec). 1st IEEE ICNP Workshop on. IEEE, 2005.
[16] Kannhavong, Bounpadith, Hidehisa Nakayama, and Abbas Jamalipour. "Nis01-2: A collusion attack against olsr-based mobile ad hoc networks." Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE. IEEE, 2006.
[17] Badis, Hakim, and Khaldoun Al Agha. "Scalable model for the simulation of OLSR and Fast-OLSR protocols." IFIP Med-Hoc-Net, Tunisia (2003).