Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.70 – 75

SURVEY ARTICLE

Analysis of Location Based Routing Protocols against Wormhole Attack for MANETs: A Literature Survey

Devendra Kumar[1], Deepak Kumar Xaxa[2]

[1]M.Tech Scholar, CSE Department, School of Engineering & IT,
MATS University, Raipur (C.G.), India
[2]Assistant Professor, CSE Department, School of Engineering & IT,
MATS University, Raipur (C.G.), India
[1] devencaught@gmail.com; [2] xaxadeepak@gmail.com

Correspondence email- devencaught@gmail.com

Abstract— The mobile nodes in MANETs dynamically change their topology and hence require an efficient mechanism to communicate with each other. There are number of routing protocols anticipated for MANET environment categorized as Location based routing protocols and Non-Location based routing protocols. In MANETs, Location based routing protocols are preferred as they are more efficient in routing compared with the Non -Location Based routing protocols. The paper presents classification of the mobile ad-hoc routing protocols and survey of location based routing protocols against wormhole attack.

Keywords— MANETs, Routing Protocols

I. INTRODUCTION

MANETs stands for Mobile Ad hoc networks where a collection of mobile hosts form a temporary network without the aid of any fixed infrastructure or centralized management. A MANET is referred to as an infrastructure-less network because the mobile nodes in the network communicate with each other using a wireless physical medium without relying on pre-existing wired infrastructure. In a MANET, nodes communicate directly with other nodes within their transmission range; however nodes outside transmission range have to depend on some other nodes to relay the messages. Thus it leads to a multi-hop scenario, where several intermediate nodes relay the packets sent by the source node before they reach to the destination node.

The function of a routing protocol in ad-hoc network is to establish routes between different nodes. Ad-Hoc routing protocols are not easy to design in general. There are two main reasons for this: the highly dynamic nature of these networks due to the high mobility of the nodes and the need to operate efficiently with limited resources such as network

bandwidth, the limited memory and battery power of the individual nodes in the network. In addition, routing protocols in ad-hoc networks face problems to work well due to frequently varying network topology, not having predefined infrastructure like routers, peer-to peer mode of communication and restricted transmission communication range.

However many routing protocols which are compatible with the characteristics of ad-hoc networks have been anticipated. They can be classified into two main categories: non-location based (topology based) and location-based (geographical or position based). Non location based routing protocols use information about links that exist in the network to perform packet forwarding. In general, non-location based routing protocols do not perform well in these networks with more than hundred nodes.

In recent developments of routing protocols, location-based routing protocols exhibit better scalability, performance and robustness against frequently changing topology of the networks. Location-based routing protocols use the geographical position of nodes to make routing decisions, which results in enhanced efficiency and performance. These protocols need that a node be able to obtain its own geographical position and the geographical position of the destination node. This information is obtained by means of Global Positioning System (GPS) and location services. The routing decision at each node is made based on the destination's position contained in the packet and the position of the neighbour nodes. There are different kinds of position-based protocols which are categorized into two main groups: location service and forwarding strategy protocols.

Another open research issue for MANETs is its security against severe type of attacks. Security is particularly more challenging due to its nature of communication and lack of infrastructure support. A number of security mechanisms has been developed and proposed, but still it is difficult to ensure that whole network is free from any malicious attack. According to the root causes of the attackers, they can be divided into internal attack and external attack. External attack (EA) is launched by external illegal node or malicious node. Internal attack (IA) is launched by the internal node and is usually from an internal network. Also IA belongs to the compromising nodes inside the network which are actually protected by network defence mechanism, so they can produce very big threat to the whole performance of the network and disable the defence mechanism. So internal attack is more effective than external attack and it is uneasy to be stopped. Wormhole attack is a kind of special internal attack for which routing protocol is the lack of effective defence mechanism to this kind of attack.

This paper is concentrated on the routing as well as security issues of MANETs associated with the location based routing protocol and wormhole attack. The rest of this paper is organized as follows: Section 2 introduces classification of routing protocols, Section 3 describes location based routing protocols and Section 4 has conclusion.

II. CLASSIFICATION OF ROUTING PROTOCOLS

The routing protocols are classified into following categories based on their fundamental architectural framework as follows:

(i) Non-Location based Routing Protocols

A. Reactive Protocols (On-demand)

These types of protocols create route only when the source requests a route to a destination .They create a route through a route discovery procedure. In which route request packets are flooded throughout the network starting with the immediate neighbours of the source. Once a route is fashioned or numerous routes are found for the destination, the route discovery process comes to an end .A route maintenance procedure maintains the continuity

of the route for the time span it is needed from the source. Some of the examples of the reactive routing protocols are DSR, AODV, and TORA etc.

B. Proactive Protocols (Table-driven)

In networks utilizing a proactive routing protocol, each node maintains one or more tables on behalf of the entire topology of the network. These tables are restructured repeatedly in order to preserve up-to-date routing information from each node to every other node. To preserve the up-to-date routing information, topology information requests to be exchanged between the nodes on a ordinary basis, leading to comparatively high overhead on the network. On the other side, routes will always be available on request. Examples of proactive routing protocols are DSDV and FSR protocols.

C. Hybrid Protocols

The hybrid protocol uses a combination of reactive and proactive approach to maintain routes. In the hybrid technique proactive approach is used when the nodes are in the local neighbourhood i.e. for the nodes up to a certain hops and reactive approach is used when the destinations nodes are far away. Example is ZRP.

(ii) Location based Routing Protocols (Geographical or Position based)

These types of protocols assume that the individual nodes are aware of the locations of all the nodes within the network .The best and easiest technique is the use of the Global Positioning System (GPS) to determine exact coordinates of these nodes in any geographical location. This location information is then utilized by the routing protocol to determine the routes. Some examples of location aware routing protocols are LAR, DREAM, GPSR, ALERT etc. The main prerequisite for location based routing is that a sender can obtain the current position of the destination. Typically, a location service is liable for this task.

III. LOCATION BASED ROUTING PROTOCOLS

Ko and Vaidya [2] presented Location-Aided Routing (LAR) protocol which uses the location information to identify the request zone and expected zone. Request zone in this protocol is the rectangular area including both senders as well as receive. By declining the search area, this protocol leads to the decrease in routing overheads.

Zaruba, Chaluvadi and Suleman [3] proposed LABAR (Location Area Based Ad-hoc Routing) protocol. It requires only a subset of nodes to know their exact location forming location areas around these nodes. Nodes that are enabled with GPS equipment are referred to as G-nodes. G-nodes are interconnected into a virtual backbone structure to enable efficient exchange of information for the mapping of IP addresses to locations. This protocol is a combination of proactive and reactive protocols, because a virtual backbone structure is used to disseminate and update location information between G-nodes, while user packets are relayed using directional routing towards the direction zone of the destination.

Karp and Kung [4] proposed GPSR (Greedy Perimeter Stateless Routing) which uses the location of node to forward the packets on the basis of distance. The packets are forwarded on a greedy basis by selecting the node closest to the destination. This procedure continues until the destination is reached. In some cases the best path may be through a node which is farther in distance from the destination node. In such scenario right hand rule is applied to forward around the obstacle and resume the greedy forwarding as soon as possible.

Tzay and Hsu [5] presented a location based routing protocol called LARDAR. Firstly, it uses the location information of destination node to predict a smaller triangle or rectangle

request zone that covers the position of destination in the past. The lesser route discovery space reduces the traffic of route request and the probability of collision. Secondly, in order to adapt the exactness of the estimated request zone, and reduce the searching range, it applied a dynamic adaptation of request zone technique to trigger intermediate nodes using the location information of destination node to redefine a more precise request zone. Finally, an increasing –exclusive search approach is used to redo route discovery by a progressive increasing search angle basis when route discovery failed.

Mohammad A. Mikki [6] introduced an Energy Efficient Location Aided Routing (EELAR) Protocol for MANETs that is based on the Location Aided Routing (LAR). EELAR makes significant reduction in the energy consumption of the mobile nodes batteries by limiting the area of discovering a new route to a smaller zone. Thus, control packet overhead is considerably condensed. In EELAR a allusion wireless base station is used and the network's circular area cantered at the base station is divided into six equal sub-areas. At route discovery as an alternative of flooding control packets to the whole network area, they are swamped to only the sub-area of the destination mobile node. The base station provisions locations of the mobile nodes in a position table.

Karim El Defrawy and Gene TsudikIn [7] addressed some interesting issues arising in suspicious MANETs by designing an anonymous routing framework (ALARM). It uses node's current locations to construct a secure MANET map. Based on the recent map, every node can decide which other nodes it wants to communicate with. ALARM takes benefit of some advanced cryptographic primitives to achieve node verification, data integrity, anonymity and intractability (tracking-resistance). It also offers opposition to certain insider attacks.

Haiying Shen and Lianyu Zhao [8] proposed an Anonymous Location-based Efficient Routing protocol (ALERT) to offer high anonymity protection at a low cost. ALERT dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which structured a non-traceable anonymous route. Furthermore, it hides the data initiator/receiver among many initiators/receivers to reinforce source and destination anonymity protection. ALERT achieves better route anonymity protection and lower cost compared to other anonymous routing protocols. Also, ALERT achieves analogous routing effectiveness to the GPSR geographical routing protocol.

Mohammad Al-Rabayah and Robert Malaney [9] introduced a new hybrid wireless routing protocol specifically designed to address this issue. This protocol combines features of reactive routing with location-based geographic routing, in such a manner so as to efficiently use all the location information available. The protocol is designed to gracefully exit to reactive routing as the location information degrades. Another aspect of this protocol is that it can be spatially dependent – meaning different physical areas of the network can be using quite different routing procedures at the same epoch. This protocol can dramatically increase scalability can be measured via the routing control overhead.

Dan Luo and Jipeng Jhou [10] proposed an improved Hybrid Location based routing Protocol approach combines geographic routing with topology based routing protocol. It over comes the major problems of reactive routing and the end-to-end delay is reduced by this algorithm. In addition, the path length performance of geographic routing is also improved. This routing protocol outperforms the pure reactive routing in terms of average delay and packet delivery rate.

Lee, Yoo and Kim [11] proposed a mechanism that considers not only the location of nodes but energy consumption to solve the several problems in wireless networks by improving LAR algorithm. This protocol provides efficient routing by minimizing the flooding of unnecessary control message, considering the limited energy of a mobile node and using appropriate transfer power to communicate. Proposed scheme can reduce energy

consumption and the average lifetime increases 12 percent than Location Aided Routing Protocol.

Shanshan, Yanliang, Yonghe, Mohan [12] proposed LOOP (A Location Based Routing Scheme for Opportunistic Networks), a new location based routing scheme for opportunistic networks. By forwarding messages to specified location instead of a targeted node, LOOP can serve as the underlying routing protocol for a plethora of pervasive applications. This protocol effectively employs node's movement patterns that are learnt from mobility trace in message forwarding. They evaluate the performance of LOOP and compare with well known protocols including Epidemic, Prophet and Bubble Rap. The Proposed scheme is able to deliver messages at a high ratio; drastically reduce network load and nodes' buffer occupation, especially when more messages are involved in the network.

Prakash Raj, Selva Kumar, Lekha [13] proposed protocol LBRP (Location-Based Routing Protocol) for ad hoc networks based on location system .The aim is extracting an optimum topology from the dynamic and irregular topology of a mobile ad hoc network to reach more quickly the destination applying for routing. The method operates in a loop free manner.

Kim, Young-Song, Hwang [14] proposed the locationbased routing algorithm that is possible to have a stable data transmission with less energy consumption. The proposed technique does not ask for the BS to be aware of locations of nodes and tries to consume balanced distributed energy of all nodes through the Lifecycle of the network. It also operates location-based routing algorithm which transmits location information of node with cluster based to widen extension and mobility and makes itself possible to apply to the distributed environment network.

Haidar Safa, Hassan Artail and Diana Tabet [15] proposed a novel cluster based trust-aware routing protocol (CBTRP) for MANETs to protect forwarded packets from intermediary malicious nodes. The anticipated protocol organizes the network into one-hop disjoint clusters then elect the most qualified and trustworthy nodes to play the role of cluster-heads that are responsible for handling all the routing activities. The anticipated CBTRP continuously ensures the trustworthiness of cluster-heads by replacing them as soon as they become malicious and can dynamically update the packet path to avoid malicious routes.

Putthiphong Kirdpipat and Sakchai Thipchaksurat [16] presented the impact of mobility on a scheme called Location-based Routing with Adaptive Request Zone (LoRAReZ). In LoRAReZ, the size of expected zone and request zone is set adaptively based on the distance between the source node and destination node. Proposed protocol evaluates the impact of mobility on the performance of LoRAReZ in terms of packet delivery fraction, routing overhead, end-to-end delay, and throughput and power consumption by comparing with those of the traditional AdHoc On-Demand Distance Vector (AODV) and Modified Ad Hoc On-Demand Distance Vector (MAODV).

Juanfei Shi and Kai Liu [17] proposed PLCR (A power efficient location-based cooperative routing algorithm) to reduce the overall power for routing in wireless networks. With hypothetical analysis, by means of a cooperative relay, the likelihood of successful packet reception can be enlarged, and the overall power for routing can be condensed, given the outage probability of the link controlled at a definite objective level. PLCR algorithm uses the location information of nodes to select the finest next-hop node and supportive node hop by hop with minimum power so that the cooperative route with minimum overall power from source to destination can be set up. PLCR routing algorithm considerably reduces the overall power in comparing to non-cooperative routing algorithm.

IV. CONCLUSION

The paper introduces different categories of ad-hoc routing protocols and reviewed several locations based routing protocols. These Location based routing protocols differ with each other in a ways of finding and maintaining the routes b/w source to destination but share the common aim of reducing control packet overhead ,maximize throughput, minimize the power consumption and end-to end delay.

Previously, very little attention has been given on addressing location based routing protocols against wormhole attack. As location based routing protocols are better in routing comparing with the non-location based routing protocols, so there is a need of securing such routing protocol against severe security attacks by analyzing stronger attacks like wormhole attack.

REFERENCES

[1] Devendra Kumar and Deeoak kumar Xaxa, "***Effectiveness of Location Based Routing Protocols against Wormhole Attack in MANETs***", *International Journal of Engineering and Computer Science (IJECS), Volume 3 Issue 5, Page No. 5588 -5593, ISSN: 2319 -7242, May-2014.*

[2] Y.B. Ko and N. H. Vaidya, "Location-Aided Routing in Mobile Ad Hoc-Scale for Ad Hoc Networks," Proceedings of the second ACM international symposium on Mobile ad hoc networking & computing, Long Beach, CA, USA, Wireless Networks (6)307–321, 2000.

[3] Gergely V. Záruba, Vamsi K. Chaluvadi, and Azeem M. Suleman, "LABAR: Location Area Based Ad Hoc Routing for GPS-Scarce Wide-Area Ad Hoc Networks"IEEE;00, 2003,7-7669955-1-1889953;0-13.

[4] B. Karp and H. Kung,. "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks" in: Proceedings of ACM MobiCom, 2000, pp. 243–254.

[5] Tzay-Farn Shih and Hsu-Chun Yen, "Location-aware routing protocol with dynamic adaptation ofrequest zone for mobile ad hoc networks", Springer Wireless Network,14:321–333,DOI 10.1007/s11276-006-9955-y, 2008.

[6] Mohammad A. Mikki, "Energy Efficient Location Aided Routing Protocol for Wireless MANETs" International Journal of computer science and Information Security, Vol. 4, No.1 & 2, pp 331-337, 2009.

[7] Karim El Defrawy, Member, and Gene Tsudik, Senior Member,"Privacy-Preserving Location-Based On-Demand Routing in MANETs" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, (29): 10,1926-1934, 2011.

[8] Haiying Shen and Lianyu Zhao ALERT, "An Anonymous LocationBased Efficient Routing Protocol in MANETs" IEEE TRANSACTIONS ON MOBILE COMPUTING, 2013, (12) 6:1079-1093.

[9] Mohammad Al-Rabayah, Robert Malaney, "A New Hybrid Location-based Ad Hoc Routing Protocol" IEEE Communications Society subject matter experts for publication, 978-1-4244-5638-3/10, 2010.

[10] Dan Lue & Jipeng Jhou,."An Improved Hybrid Location Based Routing Protocol For Ad-H0c network" IEEE Network,978-1-4244-6252, Nov-2011.

[11] Jangsu Lee, Seunghwan Y00, and Sungchun Kim, "Energy aware Routing in Location based Ad-hoc Networks"Proceedings of the 4th International Symposium onCommunications, Control and Signal Processing, ISCCSP, 978-1-4244-6287-2, 3-5, Mar-2010.

[12] Shanshan Lu, Yanliang Liu, Yonghe Liu and Mohan Kumar, "A Location Based Routing Scheme For Opportunistic Networks" IEEE Netwok, 978-1-4673-2433, 2012.

[13] Dr. E. George Dharma Prakash, Raj, S. Selva Kumar and R. Lekha,"LBRP: GEOGRAPHIC ROUTING PROTOCOLS FOR MANETs" IEEE-International Conference on Recent Trends in Information Technology, ICRTIT, 2011, 978-1-4577-0590.

[14] Jin-I Kim, Jeong-Young Song, Yoon-cheol Hwang, "Location-based Routing Algorithm Using Clustering in the MANET" Future Generation Communication and Networking (FGCN),2007, (2): 527 – 531,0-7695-3048-6.

[15] Haidar Safa ,Hassan Artail and Diana Tabet, "A cluster-based trustaware routing protocol for mobile ad hoc networks" Springer Science Business Media, LLC, 16:969–984, DOI 10.1007/s11276-009-0182-1, 2010.

[16] Thipchaksurat Sakachai and Putthiphong Kirdpipat "Impact of Mobility on Location-based Routing with Adaptive Request Zone in Mobile Ad-hoc Networks" IEEE Network, 2012, 978-1-4673-2025.

[17] Juanfei Shi and Kai Liu, "Power-efficient Location-based Cooperative Routing in Wireless Networks" IEEE Network, 2012, 978-1-4673-0199, pp. 1454-1458.

