International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 3 Issue 7 July 2016

Analysis of Various Routing Protocol in Mobile Ad Hoc Networks

Mohd. Alhaz[1], Faisal Qamar[2]
Research Scholar, Al Falah university[1, 2]
alhazkhan@gmail.com[1]

Abstract: *To facilitate communication within the network a routing protocol is used to discover routes between nodes. The goal of the routing protocol is to have an efficient route establishment between a pair of nodes, so that messages can be delivered in a timely manner. Mobile ad hoc networks (MANETs) can be defined as a collection of large number of mobile nodes that form temporary network without aid of any existing network infrastructure or central access point. Each node participating in the network acts both as host and a router and must therefore is willing to forward to packets for other nodes. The characteristics of MANETs such as: dynamic topology, node mobility, provides large number of degree of freedom and self-organizing capability of that make it completely different from other network. Due to the nature of MANETs, to design and development of secure routing is challenging task for researcher in an open and distributed communication environments. The main work of this paper is to address the security issue, because MANETs are generally more vulnerable and we proposed a secure routing protocol for MANETs, are named Hybrid based on ZRP (zone routing protocol). This protocol is work on various modes; each mode corresponds to specific state of the node. This protocol is design to protect the network from malicious and selfish nodes. We are implementing Extended Public key Cryptography mechanism in ASRP in order to achieve security goals.*

Keywords: *MANETs, WSN, ZRP, DSDV, DSR, OSLR.*

1. INTRODUCTION

Mobile ad hoc networks represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self organize into arbitrary and temporary adhoc network topologies. Wireless network has become very popular in the computing industry. Wireless network are adapted to enable mobility. There are two variations of mobile network. The first is infra-structured network (i.e. a network with fixed and wired gateways). The bridges of the network are known as base stations. A mobile unit within the network connects to and communicates with the nearest base station (i.e. within the communication radius). The second type of network is infrastructure less mobile network commonly known as AD-HOC network. They have no fixed routers. All nodes are capable of moving and be connected in an arbitrary manner. These nodes function as routers, which discover and maintain routes to other nodes in the network. Some applications of ad-hoc network are using by laptop to participate in an interactive lecture, business associates sharing information during a meeting, soldiers relaying information about situation awareness in a battlefield, and emerging disaster relief after an earthquake or hurricane. An ad-hoc network is a collection of mobile nodes, which forms a temporary network without the aid of centralized administration or standard support services regularly available on conventional networks. The nodes are free to move randomly and organize themselves arbitrarily; thus the network's wireless topology may change rapidly and unpredictably.

Infrastructure Wireless Networks

In this architecture that allow the wireless station to make a communication between each other and this type relies on the third fixed party and we call it a Base Station and that will hand-over the offered traffic from the Station to another, same entity will regulate or organize the allocation of radio

resources. Although a source node likes to communicate with a destination node, former notifies the base station. At this point, communicating nodes do not need to know anything about the route from one to another. All that matters is that the both the source and the destination nodes are within the transmission range for the Base Station and then if there's any one loses this condition, the communication will frustration or abort.

Infrastructure less Wireless Networks

The mobile wireless network as is well known an Ad Hoc Network MANETs, it has been previously defined in the Bidder is a collection of two or more devices or nodes or terminals with wireless communications and networking capability that communicate with each other without the aid of any centralized administrator also the wireless nodes that can dynamically form a network to exchange information without using any existing fixed network infrastructure. It's an autonomous system in which mobile hosts connected by wireless links are free to be dynamically and sometime act as routers at the same time. The infrastructure less it's important approaches in this technique to communication technology that supports truly pervasive computing widely duo to there's a lot of context information need to exchange between mobile units cannot rely on the fixed network infrastructure but in this time the communication wireless became develops very fast.

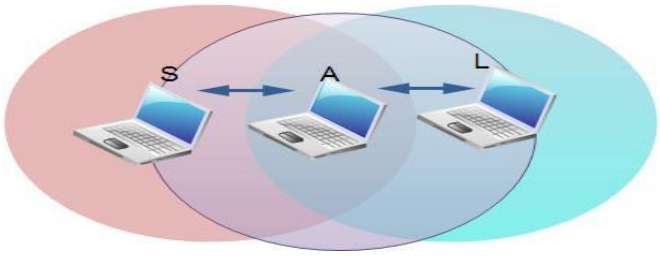

Figure 1 Illustration of the infrastructure less networks (Ad Hoc Networks).

MANET Architecture

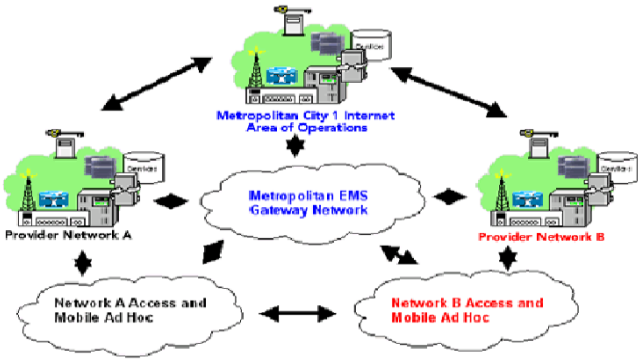

Figure 2 MANET Architecture.

Mobile Ad-hoc networks are self-organizing and self-configuring multi hop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multi hop forwarding. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network.

In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets; a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes.

2. CLASSIFICATION OF ROUTING PROTOCOLS IN MANET'S

Classification of routing protocols in MANET's can be done in many ways, but most of these are done depending on routing strategy and network structure. According to the routing strategy the routing protocols can be categorized as

Table-driven and source initiated, while depending on the network structure these are classified as flat routing, hierarchical routing and geographic position assisted routing. Both the Table-driven and source initiated protocols come under the Flat routing.

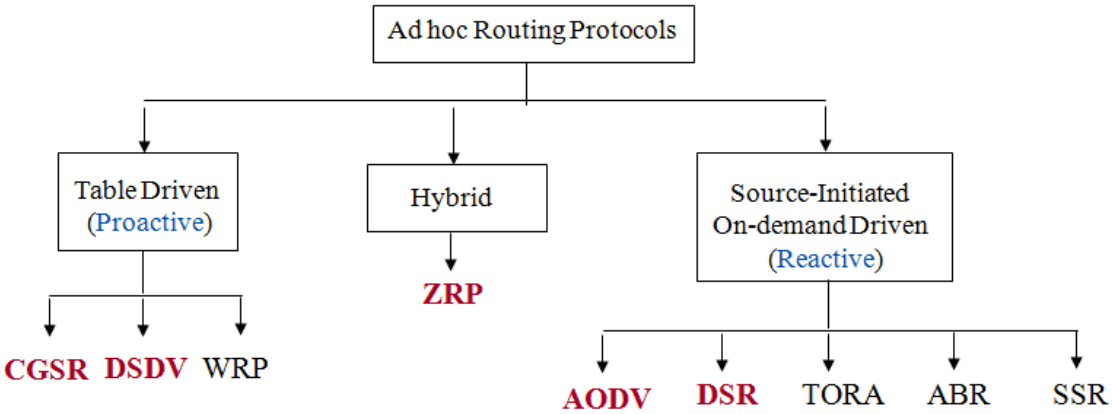

Figure 3 Classification of Adhoc Routing Protocols

Table-Driven routing protocols (Proactive)

These protocols are also called as proactive protocols since they maintain the routing information even before it is needed. Each and every node in the network maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes. Many of these routing protocols come from the link-state routing. There exist some differences between the protocols that come under this category depending on the routing information being updated in each routing table. Furthermore, these routing protocols maintain different number of tables.

On Demand routing protocols (Reactive)

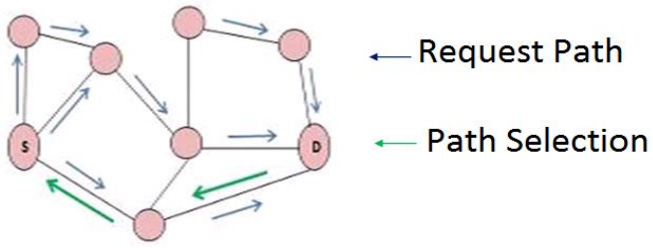

Figure 4 Route Discovery process in AODV

These protocols are also called reactive protocols since they don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network there are two advantage of on demand routing protocol.

1. High latency time in route finding.
2. Excessive flooding can lead to network clogging.

Hybrid Routing Protocols

This type of protocol combines the advantages of proactive and reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice of one or the other method requires predetermination for typical cases. The main disadvantages of such algorithms are:

1. Advantage depends on number of other nodes activated.

2. Reaction to traffic demand depends on gradient of traffic volume.

Examples of hybrid algorithms are:

1. ZRP (Zone Routing Protocol)[6] ZRP uses IARP as pro-active and IERP as reactive component.
2. ZHLS (Zone-based Hierarchical Link State Routing Protocol)

For example, reactive routing protocols are well suited for networks where the call-to-mobility ratio is relatively low. Proactive routing protocols, on the other hand, are well suited for networks where this ratio is relatively high. The performance of either class of protocols degrades when the protocols are applied to regions of ad hoc networks space between the two extremes.

3. GENERAL ATTACKS ON AD HOC NETWORK ROUTING PROTOCOLS

Attacks on an ad hoc network routing protocols generally fall into one of two categories: routing disruption attacks and resource consumption attacks. In a routing disruption attack, the attacker attempts to cause legitimate data packets to be routed in dysfunctional ways. In a resource consumption attack, the attacker injects packets into the network in an attempt to consume valuable network resources such as bandwidth, or to consume node resources such as memory (storage) or computation power. From an application layer perspective, both attacks are instances of a Denial-of-Service (DoS) attack.

Security Issues:

Mobile wireless networks are generally more prone to security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. Snooping is unauthorized access to another person's data. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

In network layer wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel.

In Black hole attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created [7].

4. CONCLUSION

In moving forward towards fulfilling the opportunity, the successful addressing of open technical and economical issues will play a critical role in achieving the eventual success and potential of MANET technology. Despite the large volume of research activities and rapid progress made in the MANET technologies in the past few years, almost all research areas (from enabling technologies to applications) still harbor many open issues. This is characteristically exemplified by research activities performed on routing protocols. Most work on routing protocols is being performed in the framework of the IETF MANET working group, where four routing protocols are currently under active development. Finally we have identified possible applications and challenges facing ad-hoc wireless networks. While it is not clear that any particular algorithm or class of algorithm is the best for all scenarios, each protocol has definite advantages and disadvantages and has certain situations for which it is well suited. The field of

ad-hoc mobile networks is rapidly growing and challenging, and while there are still many challenges that need to be met, it is likely that such networks will see wide-spread use within the next few years.

REFERENCES

[1] Johnson, D.B., and D.A. Maltz, 1996. Dynamic source routing in adhoc wireless networks, in: T. Imielinski, H. Korth (Eds.), Mobile Computing, Kluwer Academic Publishers, pp. 153–181.
[2] Perkins, C.E., and E.M. Royer, 1999. Ad-hoc on demand distance vector routing, in: Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100.
[3] Dube. R., et. al., 1997. Signal Stability based Adaptive Routing (SSA) for AdHoc Mobile Networks, IEEE Pers., Communication, pp. 36-45.
[4] S. Yi, P. Naldurg, and R. Kravets, Security-aware ad hoc routing for wireless networks. In Proc. ACM Mobihoc, 2001.
[5] L. Zhou and Z. J. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, 1999.
[6] K. Mandalas, D. Flitzanis, G. F. Marias, P. Georgiadis, "A Survey of Several Cooperation Enforcement Schemes for MANETs", 2005 IEEE.
[7] Mohammed Zeshan, Shoab A. Khan, Ahmad Raza Cheema, Attique Ahmed, "Adding security against Packet Dropping Attack in Mobile Adhoc Networks", ISBN 978-0-7695- 3480-0 @ 2008 IEEE.
[8] Srdjan Capkun, Jean- Pierre Hubaux, "BISS: building secure routing out of an incomplete set of security associations", ISBN:1-58113-769-9 @ 2003.
[9] S. Murthy and J. J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183–97.