International Journal of Advanced Science and Research
ISSN: 2455-4227
Impact Factor: RJIF 5.12
www.allsciencejournal.com
Volume 3; Issue 1; January 2018; Page No. 137-140

A review on various intrusion and path establishment routing protocols in MANET

Varun Maini
Assistant Professor, Department of Computer Science & Applications, S.U.S. Panjab University Constituent College Guru Harsahai, Punjab, India

Abstract
MANET is the field of communication that has been used for communication over the network. MANET is state free that has no structure for information sharing. In MANET nodes that have been mobile in nature has been act as sender as well as gateway for message forwarding. In this process of MANET various approaches have been used for message transmission. In this paper a review has been done that has been used for data transmission from sender to destination. Routing protocol is responsible for path establishment that is based on proactive and reactive routing. Various routing protocol has been designed that are used for malicious node detection and data communication on the network. In this paper a study has been discussed about these routing protocols.

Keywords: AODV, MANET, DSR, CBDS and DSDV

1. Introduction

1.1 Mobile Ad Hoc Network (MANET)

MANETs stand for Mobile Ad hoc Networks. Mobile implies "mobility". Ad hoc is a Latin word and it means "for this only". MANET is a collection of mobile routers or nodes that communicate over wireless network.

MANET is a less IP based network of mobile and wireless machine nodes connected with radio. In operation, the nodes of a MANET do not have any centralized administration mechanism. It is known for its network properties where each node acts as a "router" to forward the traffic to other particular node in the network very fatly.

MANET is an Infrastructure containing less wireless network. The routers or nodes moves dynamically and organize themselves randomly. The nodes directly communicate through wireless links with each other's, while that are distant apart use other nodes as relay in a multi-hop routing function. As the nodes are mobile, the structure of the network changes randomly over time. Ad-hoc networks are self-configuring and self-organizing, so to maintain communication between nodes in the network, each node behaves as a transmitter etc.

1.2 Characteristics of MANET

- MANETs do not have any central authority; unlike the traditional network makes MANET decentralized system.
- MANETS connects themselves by discovering the topology and deliver the messages themselves makes MANET a self-configuring network
- Mobile nodes in the MANET are free to take random movement. This will result frequent changes in the topology, where alternative paths are found automatically, by own self. They use different routing mechanisms in transmitting the data packet to the desired nodes by this it exhibits dynamic topology.
- MANET usually operates in bandwidth-constrained variable-capacity links. That in the result of high bit errors, low bandwidth, unstable and asymmetric links results in congestion problems.
- Power conservation plays a key role in MANET as the nodes involved in this network generally uses exhaustible battery/energy sources this makes MANETS energy-constrained.
- Finally, Mobile wireless networks are more vulnerable to eavesdropping and interception. Network control will increase the robustness of the failure, rather than centralized network dispersion.

1.3 Routing Protocol used in MANET

The main goal of routing protocols in ad-hoc network is to establish optimal path (minimum hops) between source and destination and minimum overhead and minimum bandwidth consumption so that packets are delivered in a timely manner. Routing is an activity that is used for packet send from source to destination in the network. Routing activities are established an optimal routing paths and transferring the Packets in the internetwork. Routing protocols can be divided into three categories.

1. Proactive routing protocol
2. Reactive routing protocol
3. Hybrid routing protocols

1.3.1 Proactive Routing Protocol

Proactive Routing Protocol, every node in proactive routing maintains one or more tables and representing the entire topology of the network. These tables are updated regularly and maintain up-to-date routing information from each and every node. To maintain the up-to date routing information, topology information needs to be exchanged between the nodes on a regular basis, create to relatively high overhead on the network. In proactive routing, routes will always be

available on request. The periodically to broadcast messages, so a waste of wireless bandwidth and wireless node power. Proactive routing protocols are also called as table driven routing protocols. In this each node maintain routing table which contains information about the network topology [7]. The routing tables are updated periodically whenever the network topology changes. Proactive protocols are not for large networks as they need to maintain node entries for each and every node in the routing table of every node. In proactive routing, always maintain routes, little or no delay for route determination, consume bandwidth to keep routes up-to-date, Maintain routes which may never be used.

1.3.2 Reactive routing protocol

Reactive routing protocol is called on-demand routing protocol. It is not need, maintaining routing information if there is no communication. If a node wants to send packet to another node then the protocol has to searches for the route in on demand. It has to establish the connection and transmit and receive the packet. These protocols do not maintain correct routing information on all nodes at all times. Routing information is collected only when it is needed, and route determination depends on sending route request query. The main benefit of this routing protocol is that the use of a lower bandwidth, but the drawback is that not every node that sends packets can always quickly find the path because routes are not always available. The path discovery procedure can create delays, and the average delay time is longer. In this type of protocol, route is discovered whenever it is needed. Nodes initiate route discovery when demanded. Lower overhead since routes are determined on demand and significant delay in route determination.

1.3.3 Hybrid routing protocol

Hybrid routing protocol is combination of proactive and reactive routing protocol. It overcomes the disadvantages of these protocols. This type of protocol is a trade-off between proactive and reactive protocols. Proactive protocols have more overhead and less latency while reactive protocols have less overhead and more latency [10]. Thus a Hybrid protocol is needed to overcome the shortcomings of both proactive and reactive routing protocols. This protocol is a combination of both proactive and reactive routing protocol.

1.4 Problems in Routing

Rathee discussed that routing is incorporated by several limitations as follows:

- **Asymmetric Links:** Most of the networks in which wires is used rely on the symmetric links which are always fixed. But this is not a case with Ad-hoc networks as the nodes are mobile and continuously changing their position within the network.
- **Routing Overhead:** nodes often change their location within the network. So, some stale paths are generated in the routing table which leads to unnecessary overhead.
- **Interference:** This is the major problem with MANETs as links come and go depending upon the transmission characteristics, one data transmission might interfere with another one and node might overhear transmissions of other nodes and can corrupt the total data transmission.
- **Dynamic Topology:** Since the topology is not constant, so the mobile node might move or medium characteristics might change. In Ad-hoc networks, routing table must somehow reflect the changes in the topology and routing algorithms have to be adapted.

2. Review of Literature

Sridhar (2010) in the paper "A Survey on QoS Based Routing Protocols for MANET" presents an overview and comparison of existing QoS based revisions done on AODV protocol, thus providing the reader with insight into their differences and allows to highlight trends in protocol design and identify areas for future research. The review of challenges and concepts behind QoS routing in MANETs based on AODV protocol were presented. The improvements made to the protocol were analyzed. The protocols were selected in such a way as to highlight many different approaches to QoS routing in MANETs, while simultaneously covering most of the important advances in the field since the last such survey was published. This article summarized the operation, strengths, drawbacks and results of these protocols in order to enunciate the variety of approaches proposed and to expose the trends in designers' thinking. The new protocol should provide high PDR and throughput with a very short delay, less load and managing the effects of mobility. Enhancements to be done such a way the protocol proves to be best in performing routing

Kumar (2010) [10] in the paper "A Simplified Analytical Model for End-To-End Delay Analysis in MANET" presented an analytical model for average end-to-end delay that takes into account the packet reached process, back off and collision avoidance mechanisms of random access MAC between a pair of first and last node and compares the end-to-end delay experienced by a QoS AODV protocol. The proposed analytical model results closely match with the results obtained from their simulations. They investigated contention delay in a node in MANETs under symmetric conditions. Their analytical model captures a per node delay in MANETs, and the model was validated by simulations.

Jacob (2012) in the paper " Performance Analysis and Enhancement of Routing Protocol in MANET" evaluates the performance of various ad-hoc routing protocols such as DSDV, AODV, DSR, TORA and AOMDV in terms of energy efficiency and it also proposes a new routing algorithm that modifies AOMDV and it provides better performance compared to all the above protocols. Simulation is done using NS-2(version NS-2.34).

Jeetendra (2012) *et al*. in the paper "Mobile Ad hoc Network Performance Improvement Using Strategically RED" suggests RED method for improving MANET performance. Each network device has buffer for storing incoming packet if packet is not instantly transferred, store packets if buffer space is available and drop packets if buffer space is exhausted. Mobile ad-hoc Network (MANET) devices also using buffer space for same work as other network devices. MANET has its own routing protocols which can compromised with frequent route exchange, dynamic topology, bandwidth constraint and multi hop routing. Efficiently managing buffer in devices is new area for research is called Active Queue Management. AQM manages queue according to queue policy

for accepting incoming packets and forwarding received packets.

Renato *et al*. (2012) in the paper, "Interest-centric Mobile Ad-hoc Networks" described that the mobile ad hoc Networks (MANETs) pose significant shared communication medium constraints such as finite memory, number of access channels, and bandwidth to the development of effective communication protocols. Furthermore, multi-hop message forwarding multiplies the amount of simultaneous transmissions, which augment both channel contention and network congestion, increasing interference and remove protocol performance.

3. Approaches Used

CBDS Algorithm

Initially the detection mechanism is of two types, they are proactive and reactive. Proactive: proactive mechanism is to find and prevent the network from the malicious node in initial stage. Reactive: reactive mechanism is to detect that node which will be active only after the destination node finds a packet drop in the packet delivery ratio. Cooperative Bait Detection Scheme is used for preventing and detecting the black hole/gray hole attacks. A black hole attack is defined as if the source node wants to send the data packets to the destination, it losses the data packets before forwarding to the destination. The gray hole is nothing but, initially the node act as the good node, after few minutes it changed into malicious node. By using the CBDS algorithm, at first the source node will select the neighbor node with the cooperation of that node. The address of the selected node is known as bait destination address to trap the malicious node to send a request reply message. By using tracing technique the adversary node is detected and prevented. If any packet drop occurs in the packet delivery ratio, an alarm is send to the source node by the destination node to activate the detection mechanism. The CBDS scheme combines the proactive scheme to find the malicious node in the initial stage and reactive mechanism to find the adversary node later in the network.

DSR: Dynamic Source Routing (DSR)

It is a reactive protocol i.e. it doesn't utilize occasional promotions. It figures the routes when important and after that looks after them. Source routing is a routing method in which the sender of a bundle decides the complete arrangement of hubs through which the bundle needs to pass; the sender expressly records this course in the bundle's header, recognizing each sending "hop" by the location of the following node to which to transmit the packet on its way to the destination host. There are two noteworthy stages in working of DSR: Route Discovery and Route Maintenance. A host starting a course disclosure telecasts a course ask for parcel which might be gotten by those hosts inside of wireless transmission scope of it. The course asks for bundle recognizes the host, alluded to as the objective of the course disclosure, for which the course is asked. On the off chance that the course disclosure is fruitful the starting host gets a course answer parcel posting an arrangement of system jumps through which it might achieve the objective. Notwithstanding the location of the first initiator of the solicitation and the objective of the solicitation, every course ask for bundle contains a course record, in which is collected a record of the grouping of hop taken by the course demand packet as it is spread through the system amid this course disclosure.

DSDV: The Destination-Sequenced Distance-Vector (DSDV)

Routing Algorithm depends on the traditional Bellman-Ford Routing Algorithm with certain changes. Each versatile station keeps up a steering table those rundowns all accessible destinations, the quantity of jumps to come to the destination and the arrangement number doled out by the destination hub. The arrangement number is utilized to recognize stale courses from new ones and in this manner keep away from the development of circles. The stations intermittently transmit their directing tables to their prompt neighbors. A station additionally transmits its directing table if a huge change has happened in its table from the last overhaul sent. There-fore, the upgrade is both time-driven and occasion driven. The steering table upgrades can be sent in two ways: a "full dump" or an incremental overhaul. A full dump sends the full directing table to the neighbors and could traverse numerous packets though in an incremental overhaul just those sections from the directing table are sent that has a metric change subsequent to the last redesign and it must fit in a packet. In the event that there is space in the incremental overhaul packet then those sections might be incorporated who's grouping number has changed. At the point when the system is generally steady, incremental redesigns are sent to keep away from additional activity and full dump are moderately occasional. In a quick evolving net-work, incremental packet can develop enormous so full dumps will be more regular. Every course upgrade parcel, notwithstanding the directing table data, likewise contains a novel grouping number relegated by the transmitter. The course named with the most noteworthy (i.e. latest) succession number is utilized. In the event that two routes have the same succession number then the routes with the best metric (i.e. most brief course) is utilized. In light of the history, the stations appraise the settling time of routes. The stations defer the trans-mission of a directing upgrade by settling time to dispense with those redesigns that would happen if a superior route were discovered soon.

Ad hoc On-Demand Distance Vector (AODV)

AODV offers low system use and utilizes destination arrangement number to guarantee loop opportunity. It is a reactive protocol suggesting that it demands a course when required and it doesn't keep up routes for those nodes that don't effectively partake in a correspondence. A vital component of AODV is that it utilizes a destination grouping number, which compares to a destination node that was asked for by a directing sender node. The destination itself furnishes the number alongside the route it needs to take to reach from the solicitation sender node up to the destination. In the event that there are various courses from a solicitation sender to a destination, the sender brings the route with a higher grouping number. This guarantees that the ad hoc network protocol remains loop free.

4. Conclusion

MANET is self-configurable network that has been used for data transmission from source destination based on intermediate nodes available in the network. In MANET various routing protocols has been used that are based on reactive routing and proactive routing. On the basis of these routing protocols path establishment has been done so that data can be easily transmitted. On-demand routing protocols are based on RREQ and RREP process that transmit route request and various paths have been established so that on the basis of these routing protocols shortest path can be selected. CBDS is on-demand routing protocol that is based on reverse tracking process so that malicious nodes can be easily detected in the network. On the basis of study of reactive and proactive routing protocols we can conclude that on-demand routing protocol provide better data transmission over mobile network.

5. References

1. Vicomsoft. Knowledge share whitepapers wireless networking Q&A, Vicomsoft connect and protect, 2003.
2. Wikipedia. The free encyclopedia-, Mobile ad-hoc Network, http://en.wikipedia.org/wiki/Mobile_ad-hoc_ network, 2004.
3. Charles E Perkins, Elizabeth M Royer. Ad hoc on demand distance vector (AODV) routing Internet-Draft, 1998.
4. Humayun Bakht. Computing Unplugged, Wireless infrastructure, Some Applications of Mobile ad hoc networks, http://www.computingunplugged.com/issues/ issue200410/00001395001.html, 2003.
5. Loutfi, Valerie, Bruno. Securing mobile ad-hoc networks, MP71 project, 2003.
6. Mario Joa-Ng, A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks, IEEE Journal on selected areas in communications, 1999, 17(8).
7. Padmini Misra. Routing Protocols for ad hoc mobile wireless Networks, http://www.cse.ohio-state.edu /~jain/cis788-99/ftp/ad-hoc routing/#TDRP, 1999.
8. Avdesh Kumar Bhatt, Chander Mohini, Shikha Thakur. A New Efficient and Reliable On-Demand Routing Protocol for MANET (ERORPM) International Journal of Advanced Research in Computer Science and Software Engineering, 2013, 3(5).
9. Anju Gill, Chander Diwaker. Comparative Analysis of Routing in MANET International Journal of Advanced Research in Computer Science and Software Engineering, 2012, 2(7).
10. Rakesh Kumar, Manoj Misra, Anil K Sarje. A Simplified Analytical Model for End-To-End Delay Analysis in MANET IJCA Special Issue on Mobile Ad-hoc Networks MANETs, 2010.
11. Al-Sakib Khan, Pathan, Hyung-Woo Lee, Choong Seon Hong. Security in Wireless Sensor Networks: Issues and Challenges ICACT, 2006.
12. Amit Shrivastava, Nitin Chander. Overview of Routing Protocols in MANET's and Enhancements in Reactive Protocols, 2013, 4-12.