Study of Attacks and Routing Protocol in Wireless Network

Sarbjeet Kaur[1] Akhilesh Bhardwaj[2]
[2]Assistant Professor
[1,2]Department of Computer Science Engineering
[1,2]SKIET, Kurukshetra University, Kurukshetra, Haryana, India

Abstract— Wireless mesh networks (WMNs) are attractive as a new communication paradigm. Ad hoc routing protocols for WMNs are classified into: (1) proactive, (2) reactive, and (3) hybrid approaches. In general, proactive routing is more suitable for a stationary network, while reactive routing is better for a mobile network with a high mobility. In many applications, a node in WMN is mobile but it can fluctuate between being mobile. Wireless mesh networks is an emergent research area, which is becoming important due to the growing amount of nodes in a network.
Key words: Wireless Network, Routing Protocol, Attacks

I. INTRODUCTION

A network in which, computer devices communicates with each other without any wire. The communication medium between the computer devices is wireless. When a computer device wants to communicate with another device, the destination device must lays within the radio range of each other. Users in wireless networks transmit and receive data using electromagnetic waves. Recently wireless networks are getting more and more popular because of its mobility, simplicity and very affordable and cost saving installation.

One of the great features of wireless network that makes it fascinating and distinguishable amongst the traditional wired networks is mobility. This feature gives user the ability to move freely, while being connected to the network. Wireless networks comparatively easy to install then wired network. There is nothing to worry about pulling the cables/wires in wall and ceilings. Wireless networks can be configured according to the need of the users. These can range from small number of users to large full infrastructure networks where the number of users is in thousands.

A wireless mesh network (WMN) is an integration result of multihop communication and wireless local area networks (LANs) technology. Wireless Mesh Networks (WMN) is a new distributed broadband access network. Compared with the typical mobile Ad hoc network, it is with less mobility and usually not powered by the battery. This feature brings many advantages to WMN, such as low up-front cost, easy network maintenance, robustness, and reliable service coverage.

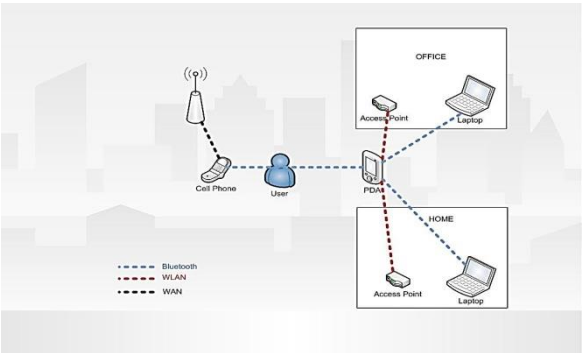

Fig. 1: Communications in Wireless Networks

II. ROUTING PROTOCOL

Routing protocols in Wireless Network are classified into three different categories according to their functionality

(1) Reactive protocols
(2) Proactive protocols
(3) Hybrid protocols

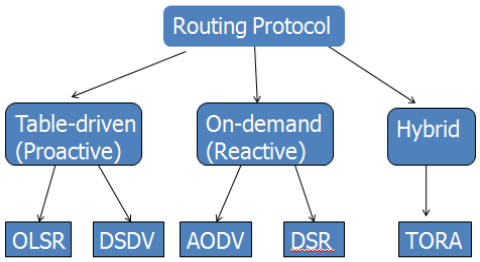

Fig. 2: Hierarchy of Routing Protocols

A. Reactive Protocol

Reactive routing protocols are on-demand protocols. These protocols do not attempt to 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 queries throughout the network. The primary advantage of reactive routing is that the wireless channel is not subject to the routing overhead data for routes that may never be used. While reactive protocols do not have the fixed overhead required by maintaining continuous routing tables, they may have considerable route discovery delay. Reactive search procedures can also add a significant amount of control traffic to the network due to query flooding. Because of these weaknesses, reactive routing is less suitable for real-time traffic or in scenarios with a high volume of traffic between a large numbers of nodes.

B. Proactive Protocol

In a network utilizing a proactive routing protocol, every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain up-to-date routing information from each node to every other node. To maintain the up-to-date routing information, topology information needs to be exchanged between the nodes on a regular basis, leading to relatively high overhead on the network. On the other hand, routes will always be available on request. Many proactive protocols stem from conventional link state routing, including the Optimized Link State Routing protocol (OLSR).

C. Hybrid Protocol

Wireless hybrid routing is based on the idea of organizing nodes in groups and then assigning nodes different functionalities inside and outside a group [13]. Both routing table size and update packet size are reduced by including in

them only part of the network (instead of the whole); thus, control overhead is reduced. The most popular way of building hierarchy is to group nodes geographically close to each other into explicit clusters. Each cluster has a leading node (cluster head) to communicate to other nodes on behalf of the cluster. An alternate way is to have implicit hierarchy. In this way, each node has a local scope. Different routing strategies are used inside and outside the scope. Communications pass across overlapping scopes. More efficient overall routing performance can be achieved through this flexibility. Since mobile nodes have only a single Omni directional radio for wireless communications, this type of hierarchical organization will be referred to as logical hierarchy to distinguish it from the physically hierarchical network structure.

III. Description Of Some Routing Protocol

A. Destination-Sequenced Distance-Vector (DSDV)

Destination-Sequenced Distance-Vector Routing protocol is a proactive table driven algorithm based on classic Bellman-Ford routing. In proactive protocols, all nodes learn the network topology before a forward request comes in. In DSDV protocol each node maintains routing information for all known destinations. The routing information is updated periodically. Each node maintains a table, which contains information for all available destinations, the next node to reach the destination, number of hops to reach the destination and sequence number. The nodes periodically send this table to all neighbors to maintain the topology, which adds to the network overhead. Each entry in the routing table is marked with a sequence number assigned by the destination node. The sequence numbers enable the mobile nodes to distinguish stale routes from new ones, there by avoiding the formation of routing loops

B. Optimized Link State Routing (OLSR)

OLSR is a proactive routing protocol, so the routes are always available when needed. The OLSR optimizes the link state algorithm by reducing the size of the control packets that contain link state information by using only selected nodes, called multi-point relay (MPR), to retransmit control messages. To select MPR, each node periodically broadcasts HELLO messages to its one-hop neighbors. Each HELLO message contains a list of neighbors that are connected to the node. Through exchanging the HELLO message, a node selects the one hop neighbors which cover all the two hop neighbors as its own MPR. In order to exchange topological information, a Topology Control (TC) message is broadcasted throughout the network. Each node maintains a routing table in which the routes for all the available destination nodes are kept.

C. Dynamic Source Routing (DSR)

Dynamic Source Routing protocol is a reactive protocol i.e. it determines the proper route only when a packet needs to be forwarded. The node floods the network with a route request and builds the required route from the responses it receives. DSR allows the network to be completely self configuring without the need for any existing network infrastructure or administration. The DSR protocol is composed of two main mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network. All aspects of protocol operate entirely on-demand allowing routing packet overhead of DSR to scale up automatically.

Route Discovery: When a source node *S* wishes to send a packet to the destination node *D*, it obtains a route to *D*. This is called Route Discovery. Route Discovery is used only when *S* attempts to send a packet to *D* and has no information on a route to *D*.

Route Maintenance: When there is a change in the network topology, the existing routes can no longer be used. In such a scenario, the source S can use an alternative route to the destination *D*, if it knows one, or invoke Route Discovery. This is called Route Maintenance.

D. Temporally-Ordered Routing Algorithm (TORA)

The Temporally-Ordered Routing Algorithm (TORA) is a distributed routing protocol for multi-hop networks with a unique approach for routing the packets to their destination. TORA is fully distributed, in that routers need only maintain information about adjacent routers (i.e. one hop knowledge) and there is no centralized control. This is essential for all Ad Hoc routing protocols. Like a distance-vector routing approach, TORA maintains state on a per-destination basis. However, it does not continuously execute shortest-path computation and thus the metric used to establish the routing structure does not represent a distance. The destination oriented nature of the routing structure in TORA supports a mix of reactive and proactive routing on a per-destination basis. During reactive operation, sources initiate the establishment of routes to a given destination on demand. This mode of operation may be advantageous in dynamic networks with relatively sparse traffic patterns since it may not be necessary or desirable to maintain routes between every source/destination pair at all times.

At the same time, selected destinations can initiate proactive operation, resembling traditional table-driven routing approaches. This allows routes to be proactively maintained to destinations for which routing is consistently or frequently required (e.g., servers or gateways to hardwired infrastructure). TORA is designed to minimize the communication overhead associated with adapting to network topological changes. The scope of TORA's control messaging is typically localized to a very small set of nodes near a topological change. A secondary mechanism, which is independent of network topology dynamics, is used as a means of route optimization and soft-state route verification. The design and flexibility of TORA allow its operation to be biased towards high reactivity (i.e., low time complexity) and bandwidth conservation (i.e., low communication complexity) rather than routing optimality-- making it potentially well suited for use in dynamic wireless networks.

IV. Description Of Some Attacks In Wireless Network

A. Gray Hole Attack

Every node maintain a routing table that stores the next hop node information for a route a packet to destination node, when a source node want to route a packet to the destination node , it uses a specific route if such a route is available in it's routing table. otherwise , nodes initiates a route discovery process by broadcasting Route Request (RREQ) message to it's neighbors. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse

route to source node. A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination.

The gray hole attack has two phases , In first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intension of interrupting or corrupting packets, event though route is spurious. In second phase ,nodes drops the interrupted packets with a certain probability. Detection of gray hole is difficult process. In some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Due this behavior it's very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack .

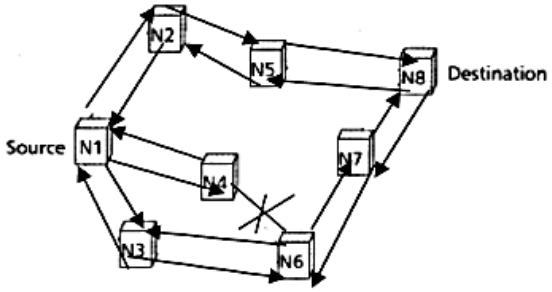

Fig. 3: Basic Idea about the Gray hole attack

B. Black Hole Attack

In this type of attack, a malicious node falsely advertises good path (e.g., shortest path or most stable path) to the destination node during the path finding process. The intension of the malicious nodes could be to hinder the path finding process or to interrupt all the data packets being sent to the concerned destination node. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it .

In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address.

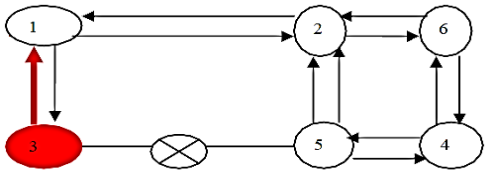

Fig. 4: Basic Idea about the Black hole attack

V. Related Work

Jing Xie, Luis Gironés Quesada and Yuming Jiang [1] proposed a Threshold-based Hybrid Routing Protocol for MANET. MANET is a network where topologies of the network changes rapidly because all the nodes are free to move and each acts as a router. In this paper a Threshold-Based Hybrid Routing protocol (THRP) had been proposed that switches between Proactive MANET Protocol (PMP) and Reactive MANET Protocol (RMP) based on the speed of the nodes. When nodes are moving slowly PMP would be running on the proactive cluster an when nodes are moving fast RMP would be running on the nodes.

In this paper theoretical comparison had been between OLSR, AODV, ZRP and THRP.OLSR consumes more bandwidth because of periodic updating of their routing table so when number of node increases overhead increases. AODV broadcast HELLO messages periodically and find routes on demand so for higher density or node mobility it may consume more bandwidth. ZRP is expected to reduce maintaince of routing table but introduces overhead because of use of proactive protocol for intra-zone. Where as THRP in PMP control flooding by defining maximum number of nodes in proactive cluster. In OLSR routes are maintained before it is required and if link broken route can be discovered rapidly so it has less delay. AODV uses on-demand route discovery so it has more delay. ZRP has lesser delay than AODV but more than OLSR especially when source and destination are in different zones. In THRP nodes within same cluster has lesser delay but if one node is of proactive cluster and other is reactive than delay increases. OLSR performance degraded as the network size increases because of overheads. AODV performance also degraded on larger network because of increased path length and delay. ZRP has zone radius which are overlapping leads to overhead flooding in other zones. THRP has better scalability than both AODV and OLSR because it uses both proactive and reactive approach and THRP is suitable for large number of moving nodes with various speeds.

Asad Amir Pirzada, Ryan Wishart and Marius Portmann[2] proposed anCongestion-Aware Routing In Hybrid Wireless Mesh Network.Multi-radio Wireless Mesh Networks (WMN) are gaining lot of popularity owing to their increased application to community and public safety networks. WMNs form a static wireless backhaul to provide connectivity to mobile clients. The wireless medium, being shared and contended for, creates a number of hurdles including congestion, interference and noise. Multiradio nodes can take advantage of the wider frequency spectrum.

However, current mesh technologies employ a simplistic approach by assigning one channel for client servicing and another for the backhaul network. The improper reuse of the same channel across multiple hops causes extensive co-channel interference leading to lower bandwidth. The problem is aggravated in a hybrid WMN where the mobile clients act as routers for other clients. In this paper, they propose a congestion aware routing protocol, which can successfully establish channel diverse routes through least congested areas of a hybrid WMN. The prime advantage of the protocol is its ability to discover optimal routes in a distributed manner without the requirement of an omniscient network entity. Simulation results show that the congestion aware routing protocol can successfully achieve a high packet delivery ratio with lower routing overhead and latency in a hybrid WMN.

Charles E. Perkins and Elizabeth M. Royer [3] proposed Ad-hoc On-Demand Distance Vector Routing , a novel algorithm for operation of ad-hoc networks. DSDV is effective for creating ad-hoc networks for small populations of mobile nodes.DSDV also requires each mobile node to maintain a complete list of routes, one for each destination within the ad-hoc network. Although AODV does not

depend specifically on particular aspects of the physical medium across which packets are disseminated.The algorithm works on wired media as well as wireless media, as long as links along which packets may be transmitted are available. The only requirement placed on the broad-cast medium is that neighboring nodes can detect each others' broadcasts.AODV uses symmetric links between neighboring nodes. It does not attempt to follow paths between nodes when one of the nodes cannot hear the other one; however we may include the use of such links in future enhancements.

Prof. Sanjeevsharma, Rajshree, Ravi PrakashPandey and VivekShukla[4] proposed Bluff—Probe based Black Hole Node Detection and Prevention. Black hole attack is easy to launch in wireless ad hoc network. Black hole attack is referred to as a node, dropping all packets and sending bogus information that it has shortest path. In black hole attack, black hole node acts like black hole in the universe. In this attack black hole node absorbs all the traffic towards itself and doesn't forward to other nodes. To attract all the packet towards it, this malicious node advertise that it has shortest path through it to the destination node. There are two types of black hole attack- Black hole attack with single malicious node- Zone with single black hole node and Black hole attack with multiple malicious node- Zone with multiple black hole nodes. In this ZRP (Zone Routing Protocol)is used. ZRP combines advantages of both proactive & reactive and makes hybrid approach. ZRP takes advantages of proactive within zone and use reactive approach when inter zone communication occurs. ZRP provide framework for routing and maintain valid route tables without too much overhead. But there is no security providence in the ZRP. Therefore SECURE-ZRP(S-ZRP) is used.

VI. WMN PROTOCOL

WMNs are of two types, reactive and proactive. In reactive routing, a route is set up whenever a communication is required. In proactive protocols, all routes between sources and destinations are investigated in advance and registered in each mesh-node routing table for future look-up. Proactive routing takes advantage of a faster path establishment when a communication is demanded; however it is not able to guarantee the required QoS, since any predefined path may go through a lot of traffic fluctuations. On the other hand, reactive routing protocols take a longer time to build up a path between a source and a destination,
as they should flood the routing information whenever communication is necessary. Therefore, they can obtain more up-to-date information about the network resources available for QoS provisioning.

A. Route Request by a Source Mesh-node

When a mesh client requests a communication, the access (source) mesh node starts route discovery by broadcasting a routing request packet whenever the RREQ packet is forwarded successfully. hop_no is initially zero and increased by one whenever RREQ advances by one hop. Bandwidth Request and service_type present the demanded bandwidth and the QoS class of the flow, respectively. minimum_bandwidth is initially set to the bandwidth Request and is overwritten whenever an intermediate mesh-node offers a lower bandwidth. As a result, minimum_bandwidth gradually presents the bottleneck of the discovered route. Finally, life_time presents the life time of the RREQ packet. The source mesh-node also setup a timer.

B. Route Request by an Intermediate Mesh-node

Upon receiving a RREQ packet, an intermediate mesh-node checks the Intermediate_nodes field to see if it has already received this packet (loop prevention). If yes, the packet will be dropped; otherwise, the node calculates the amount of bandwidth that it can offer for reservation (the corresponding algorithm will be described in the next section). The node then checks whether its offer is less than what is registered in minimum_bandwidth or not. If yes, this field will be overwritten. It also appends its own address to the intermediate_nodes field and forwards the RREQ to the neighbors. At this step, no bandwidth will be reserved. For stability reasons and adaptation with AODV routing protocol, we can also consider a maximum value for hop_no.

VII. CONCLUSION

Wireless mesh networks (WMNs) are becoming well-known as a new broadband Internet access technology through multi-hop transmission nowadays. Today, WMNs are a widely known forerunner of wireless multi-hop networking and network deployment. One of the challenging issues of the WMN is how to support real-time applications. In the past, real-time applications were mainly end-to-end communications between users.

REFERENCES

[1] Jing Xie, Luis Gironés Quesada and Yuming Jiang, "A Threshold-based Hybrid Routing Protocol for MANET" { 1-4244-0979-9/07/© 2007 IEEE}
[2] Asad AmirPirzada, Ryan Wishart and Marius Portmann, "anCongestion-Aware Routing In Hybrid Wireless Mesh Network "{ 1-4244-1230-7/07/© 2007 IEEE}
[3] Charles E. Perkins and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector Routing".
[4] Prof. Sanjeevsharma, Rajshree, Ravi PrakashPandey and VivekShukla, "Bluff-Probe Based Black Hole Node Detection and prevention"{ 2009 IEEE International Advance Computing Conference (IACC 2009 }
[5] Dong-Won Kum, Jin-Su Park, You-Ze Cho , Byoung-Yoon Cheon, and Daejea Cho, "Mobility-aware Hybrid Routing Approach for Wireless Mesh Networks" { 978-0-7695-4092-4/10 $26.00 © 2010 IEEE }
[6] Youiti Kado, Azman Osman Lim, and Bing Zhang, "Analysis Of Wireless Mesh Network Routing Protocol For Push-to-Talk Traffic "{ 1-4244-1251-X/07/©2007 IEEE.}
[7] Miguel Elias M. Campista , Lu´ıs Henrique M. K. Costa, "WPR*:* A Proactive Routing Protocol Tailored to Wireless Mesh Networks"{ 978-1-4244-2324-8/08/© 2008 IEEE.}
[8] Azzedine Boukerche, Lucas Guardalben and Joao B. M. Sobral, "Analyzed an Performance Evaluation of OLSR and AODV Routing Protocols

Using a Self-Configuration Mechanism for Heterogeneous Wireless Mesh Networks"{ 978-1-4244-2413-9/08/©2008 IEEE**}**

[9] Sheenu Sharma, Roopam Gupta, "Analyzed an Black hole Attack in AODV Routing Protocol" India, Journal of Engineering Science and Technology Vol. 4, No. 2 (2009) 243 – 250 © School of Engineering, Taylor's University College.

[10] Dong-Won Kum, Jin-Su park, You-Ze Cho, Byoung-Yoon Cheon and Daejea Cho., "Proposed an Mobility –Aware Hybrid Routing Approach For Wireless Mesh Network"{ 978-0-7695-4092-4/10 © 2010 IEEE}

