THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Cross-Layer Metrics for Reliable Routing in Wireless Mesh Networks and Understanding of OLSR and ODSBR

Ravi Kiran D.
M.Tech, Software Engineering, School of Information Technology, JNTUH, India
E. Jagadeeswararao
Lecturer, Software Engineering, School of Information Technology, JNTUH, India

Abstract*:*
Wireless Technology is used because of its suitability to mobile applications. It is mainly categorized into two types. Wireless Network with Infrastructure and Wireless Network without Infrastructure.WMN (Wireless Mesh Network) costs less to setup a network and is flexible in the network. Internet Technology is made up of logically organized layers. Mobility support cannot be implemented within a single layer efficiently so it requires cross-layer awareness and cooperation. Cross-Layer is done by allowing layers to exchange information to obtain performance gains. "Scope" defines the cross-layer approach boundaries. Cross-Layer Solutions allow interdependence and joint development of protocols. Because of the highly unstable wireless medium of WMN the design of algorithms that consider link quality to choose the best route are enabling routing metrics and protocols to evolve. "Cross-Layer Metrics" is proposed for efficient and reliable routing, identify selfish participantsand manage traffic. Cross-Layer Metrics with EFW, MEFW and JEFW metrics are used to cope up with the problem of selfish behavior of mesh routers i.e., packet dropping and are combined in a cross layer fashion with the routing layer observations of forwarding behavior with MAC Layer measurements of wireless link quality to select the most Reliable and High Performance Path. OLSR and ODSBR are explained elaborately.

Keywords*:WMN, Cross-Layer Metrics, EFW, MEFW, JEFW, OLSR, ODSBR, MAC layer*

1. Introduction

Network Elements of Mesh Network Architecture are Network Gateway, Mesh Routers and Mobile Nodes. IP table is one of the tools which can be used to easily implement packet dropping at the network layer even by a user who is not an expert. Unfairness and Performancedegradation occurs because of selfish behavior. To improve performance interaction between layers is needed. Cross- Layer is done by allowing layers to exchange information to obtain performance gains. The design and implementation of the Network is divided into Modules.Each layer performs required communication function with the help of a protocol which is implemented either by a software or hardware or firmware entity, provides services to next layer, hides the complexity of the lower layer and provides well defined services to the upper layer.

2. Literature Survey

2.1. Cross Layer

Cross-Layer is used because it easy for debugging, abstraction, design and implementation. But not favored for energy efficiency.3GPP group identified cross-layering as the approach which is able to reduce hand-off fitting the requirements of many streaming, interactive and void applications. It maintains the functionalities associated to the original layers and also allows coordination, interaction and joint optimization crossing different layers. Weak Cross-Layering involves interaction among entities at different layers of the protocol stack. Strong Cross-Layering enables joint design of algorithms implemented within any entity at any level of the protocol stack. Layers of a Network include PHY as bottom layer, MAC, Routing, Transport and Application layer as top layer. Cross-Layer signaling is divided into four types. They are Interlayer signaling pipe, Direct Interlayer Communication, Central Cross-Layer Plane, Network-wide Cross-Layer signaling. The Problems associated with this are security, non-conformant routers and processing efficiency.

<u>2.1.1. The Characteristics of Cross-Layer Signaling are</u>

- **Propagation Latency** - it describes the delay associated with signaling message delivery
- **Communication Overhead** - it describes the amount of network resources needed for signaling i.e., number of CPU cycles
- **Processing Overhead** – it is the amount of processing power required for message encapsulation, extraction, creation and analysis

- **Direction of Signaling** - it defines the applicability of signaling approach to chosen cross-layer optimization scheme
- **Requires standardization** – it specifies whether standardization effort is needed for Cross-Layering Signaling Method for full support and effective deployment

So, Cross-Layer is modeled to enable interaction among protocols operating at different layer of the protocol stack in order to improve in terms of Performance Metrics like hop count, ETT, ETX, Energy consumption, path reliability, path availability and etc.

2.2. OLSR

- **OLSR – Optimized Link State Routing Protocol** mostly used for Mobile ad-hoc networks but can be used for other wireless ad-hoc networks. It falls under Proactive link state routing protocol that floods a topology table of its neighbors to all nodes in the network which then compute optimal forwarding paths locally. It selects a route according to a specified link quality metric. It is an extension of dynamic source routing protocol. The advantages of using this protocol are less average end to end delay, implementation is more user-friendly, suitable even when have rapid changes source and destination pairs, well suited for applications which does not allow long delays in the Transmission of data packets. The disadvantages are needs more time for re-discovering a broken link, requires more processing power.
- **ETX** is used to locate a path with higher throughput in a multi-hop wireless network. It has good accuracy in determining link quality so mostly preferred routing metric. But it does not consider the bandwidth of links in a path and does not give preference to channel diversity. Also the broadcast are usually performed at Network basic rate and the probes are smaller than typical data packets.

2.2.1. Modules

Modules mostly involved in these area related projects are:

- **Network Module**
- **Real Time Packet Classification**
- **Selective Jamming Module** - Physical Layer uses a Resilient Technique such as Direct-Sequence Spread Spectrum or Frequency-Sequence Spread Spectrum is assumed
- **Strong Hiding Commitment Scheme (SHCS)** - it is used to satisfy strong hiding property while keeping Computation and Communication Overhead to a Minimum. But, Joint consideration of MAC and PHY Layers is required. They are designed so that a party cannot change the value statement after they have committed to it. They are binding
- **Cryptographic Puzzle Hiding Scheme (CPHS**) – in Cryptography, Commitment Scheme allows one to commit to a chosen value and make sure that it is not visible to others but has the ability to reveal the committed value later
- **Hiding based on all-or-nothing transformation**

2.3. ODSBR

ODSBR: On-Demand Secure Byzantine Resilient Routing Protocol is the first on-demand routing protocol that provides resilience to ‘Byzantine Attacks’ which are performed by individual or colluding attackers. Byzantine behavior is defined as any action by an authenticated node performed at Network Layer that results in degradation or disruption of the routing service i.e. on MAC/PHY Layers attacker does not have control. Services are more vulnerable to internal attacks coming from compromised nodes that behave arbitrarily to disrupt the network. Focus is on attacks at Network Layer and do not consider attacks against MAC/PHY Layers. Byzantine attack also referred to as black hole attack where the adversary drops packet selectively or entirely. The Design of ODSBR is centered around the impossibility of distinguishing between failure and malicious behavior with the capability of addressing both failure and attacks within a unified framework. ODSBR uses a ‘Secure Adaptive Probing technique’ which detects malicious links after long n faults have occurred, where ‘n’ is the length of the path. A Route Discovery mechanism which relies on a new metric that captures adversarial behavior is used to avoid problematic links. A ‘fault’ is defined as any disruption that results in significant loss or delay. Remember a Network operating normally exhibits some amount of loss. A fault is defined as a loss greater than or equal to ‘Threshold’ which is a value as low as possible. The Threshold value is determined by the source and may be varied independently for each route. Whenever the end points of a link disagree it is deduced that atleast one of them is faulty. Threshold is defined as a bound on what is considered a tolerable loss rate. Therefore, the link is considered faulty and should be avoided. The metric proposed by ODSBR captures ‘failures and adversarial behavior’ based on past history. Nodes are authenticated using public-key based techniques. Messages that cannot be authenticated are discarded. Intermediate nodes can exhibit such behavior either alone or in collusion with other nodes. Some of the Byzantine attacks are flood rushing, worm hole and overlay network worm hole. Attacks like Eavesdropping, fabricating or modifying packets can be prevented by traditional encryption, authentication and integrity mechanisms.

Upon detection of the attack i.e. the number of lost packets becomes higher than a Threshold value ODSBR enters a Probing mode with the goal of discovering the attack location. So, the location of adversary can be narrowed down to a single link. Guilt is assigned to a link. ODSBR does not use number of hops as path selection metric. Selecting the shortest path will not guarantee that such a path is adversary-free. ‘Reliability Metric’ is represented by a list of link weights where high weights correspond to low reliability. Each node contains its list referred to as weight list and dynamically updates that list when it detects faults.Faulty links are identified by a Secure Adaptive Probing Technique which is embedded in the regular packet stream and they are avoided using a Secure Route Discovery Protocol that incorporates the Reliability Metric. Route Discovery Protocol has 5 steps: They are: 1) Request Initiation - which includes source, destination, sequence number, list of detected malicious links & their weights 2) Request Propagation 3) Request Receipt or Response Initiation 4) Response Propagation 5) Response Receipt

2.4. ODSBR Involves 3 Successive Phases

- **Route Discovery in an Adversarial Environment**- which involves double flooding, per node flood verification and forwarding rules, guarantee that route discovery process will always find the low cost according to Reliability Metric.
- **Byzantine Fault Detection** – discovers problematic links on the path from the Sourceto the Destination using full path as input and outputting a faulty link. Cryptographic proof is required for the Source i.e., that packets are delivered successfully and uncorrupted to the destination in the form of secure acknowledgements. Also, probes are cryptographically coupled to every data packet, it is impossible to escape detection i.e. dropping less than an allowable Threshold.
- **Link Weight Management** - maintains a weight list for links discovered by fault detection algorithm and uses a multiplicative increase scheme to penalize links. A rehabilitation mechanism is used which limits the amount of attack or group can cause and also reduces the impact of false positives by never completely disconnecting nodes from the Network. Link Weight Management operates as follows: when a fault is registered on a link, the link’s weight is doubled. This ensures that the Protocol will eventually avoid selecting paths containing that link during future route discoveries. In addition to the weight, a counter is associated with each identified faulty link. While identifying a faulty link let µ be the number of packets dropped and p is the Threshold loss rate then the link’s counter is increased by µ/p. Each non zero counter is reduced by 1/m for every successfully delivered packet where ‘m’ is the number of links with non zero counters.

Attacks on data content like modification, Injection and eavesdropping which we assume are addressed at Data Delivery i.e. selective dropping of data or Transport or Application. ODSBR provides protection against nodes that selectively drop traffic using Detection Algorithm which is based on using authenticated acknowledgements of the data packet. Fault Detection mechanism requires to return an acknowledgment to the source for every received data packet i.e. source keeps track of losses. If the losses violate the acceptable Threshold, the Protocol registers a fault between source and the destination and starts a Binary Search on the path, in order to identify the faulty link. The interval is divided in two by insertion of a new probe, when a fault is detected on an interval. The process of sub divisionis continuedon an interval that corresponds to a single link, until a fault is detected. The link is identified as being faulty and is passed to link weight management component which will update the metric associated with the link. Shared Key Establishment is a technique proposed for on-demand creation of these keys using assumed public key infrastructure managed by a trusted Certification Authority. Generationof a new key is done for that node when the source needs to probe a node and encrypts it with that node’s public key. The encrypted key is embedded in the probe list on outgoing data packets. Once the shared key is established, acknowledgements sent by the node can be authenticated using a HMAC.

3. References

1. EFW – A Cross-Layer Metric for Reliable Routing in Wireless Mesh Networks with Selfish Participants by Stefano Paris, Cristina Nita-Rotaru, Fabio Martignon and Antonio Capone
2. A Study on Cross-Layer Metrics of Wireless Mesh Network by Swarnali Chakraborty, Abhishek Majumder
3. ODBSR: An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks by Baruch Awerbuch, Reza Curtmola, David Holmer, Christina Nita-Rotaru, Herbert Rubens
4. Cross Layer Designs in WLAN Systems edited by Prof. Nizar Zorba, Charalambos Skianis and Christos Verikoukis