An Analysis on Routing & Issues in Network Layer in WMNs

C.Gayathri, Dr.V.Kavitha

Abstract— Wireless mesh networks is composed of nodes connected in mesh architecture, hence the network is highly connected and employed in various applications. Providing end – to – end security is a tricky task since a number of attacks are present in different layers of the network. As such all the layer network layer holds the importance of routing in the network . This analysis briefly discuss about the issues in network layer of WMNs and schemes adopted for the detection of some of the network layer attacks. Denial of Service (DoS) attacks are multi layer attack they can deny service at any possible layer. Some of the DoS attacks in network layer are Blackhole Attack, Greyhole Attack. Byzantine Attack etc. A greater concern is given to network layer since the foremost duty of network layer is routing. Any attack or malfunctioning in routing causes misrouting of packets and breakdown of the network or eavesdropping of the secure information being transmitted. To mitigate the effect of such attacks different approaches are used.

Index Terms— Denial of Service (DoS), Network Layer, Routing, Detection schemes, Wireless Mesh Networks.

1 INTRODUCTION

WIRELESS MESH NETWORKS (WMNs) describes wireless networks where nodes can communicate with each other directly or indirectly through one or more nodes. WMNs are replacing wireless Infrastructure networks in many areas because of their lower cost and higher flexibility. The wireless mesh networks (WMNs) provides network access for both mesh and conventional clients through mesh routers and mesh clients. Communication across the network is formed via the bridge functions. Wireless mesh network has resolved the limitation of ad hoc networks which is ultimately improves the performance of Ad hoc networks. Nodes automatically establish an ad hoc network and maintain the connectivity. The main characteristics of WMNs include self-organization and self-healing and self- configuration.

WMNs consist of mesh routers and mesh clients. Mesh routers provide network access for both mesh and conventional clients. Mesh routers form the mesh backbone and has minimum mobility. It provides the same coverage as conventional routers do but with the lesser transmission power. It provides the additional routing functions for mesh networking. Mesh clients can be mobile or stationary as well. Mesh clients have necessary mesh functions and they can acts as a router but they do not have gateway or bridge functionality.

Depending on their functionality wireless mesh networks are classified as:

Infrastructure WMNs : Here the static mesh routers forms an infrastructure to the mesh clients that connects to them.

Client WMNs **:** Here the meshing provides peer-to-peer connectivity among the client devices. The client performs the actual routing and other functionalities.

Hybrid WMNs : This architecture is a combination of both infrastructure and client WMNs, Here the mesh clients can access the internet via mesh routers or else directly meshing through other devices.

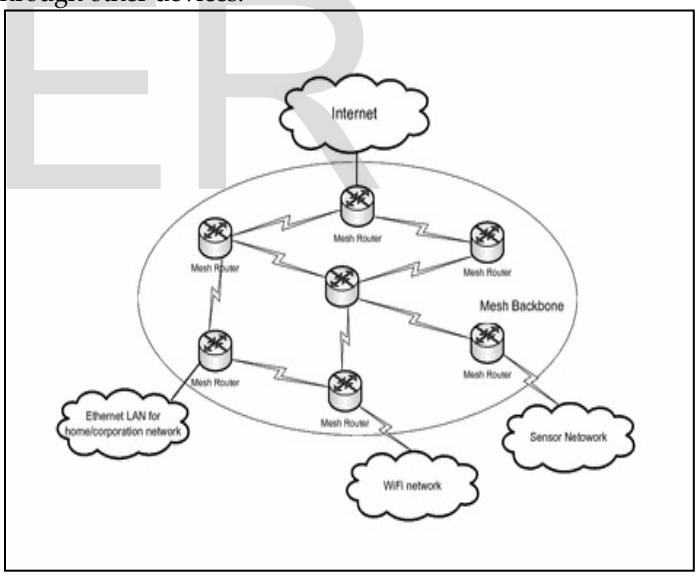

Fig 1. Wireless Mesh Network

The potential advantages of WMNs include:

- Decreased need for Internet gateways
- Collaborative redundant backup technology, which insures data security in the event of disk failure
- The ability to configure routes dynamically
- Lower power requirements, which could potentially be met by low-cost or renewable energy sources.
- Increased reliability: Each node is connected to several other nodes and if one drops out of the network, its neighbors simply find another route.

Routing in WMN extends network connectivity to end us-

C.Gayathri is currently pursuing her M.E in Communication systems in M.Kumarasamy College of Engineering, Karur; Email ID : gayathrichandrasekar92@gmail.com

Dr.V.Kavitha is Professor & HOD – ECE in M.Kumarasamy College of Engineering, Karur; Email ID : emiroece@gmail.com.

ers through multi-hop relays including the access points and the network gateways. This ultimately should be done while optimizing network resource utilization and accommodating users QoS requirements. The shared medium characteristics and varying link capacity are some of the crucial design constraints in WMN routing. Unlike ad hoc routing, WMN routing involves primarily a fixed backbone consisting of both non energy constrained nodes (i.e., access points and network gateways), and mobile energy-constrained wireless nodes (i.e., mobile devices) may also be considered.

The Key Benefits of a Wireless Mesh Network over ad-hoc network are**:**

1) *Less Expensive than Traditional Network* - The wireless mesh network is used particularly for large areas of coverage. The wireless mesh networks can reduce the cost and complexity of installing fiber/wires between buildings.

2) *Wireless Mesh is mostly adaptable and expandable* - Wireless Mesh is very useful for those areas where there is lack of sight or where network configurations are intermittently blocked. With wireless mesh, adding more wireless mesh nodes will adjust to find a clear signal. Wireless mesh is also extremely suitable where wall connections may be lacking.

3) *Wireless mesh networks support high demand* - public safety and emergency response demands wireless connectivity that supports coverage of big geographic areas and high quality video surveillance. Wireless mesh networks are perfect to deliver high throughput and faster wireless connectivity. [20].

2 Network Layer

Despite the availability of many routing protocols for WMNs, the designing of routing protocols for WMNs is still an active research area. The most approving routing protocol for WMNs must capture the following features:

- **Multiple Performance Metrics.** Many proposed protocols use minimum hop-count as a performance metric to select the routing path. This has been confirmed to be ineffective in many situations.
- **Scalability.** Setting up or maintaining a routing path in a very large wireless network may take a long time. Thus, it is vital to have a scalable routing protocol in WMNs.
- **Robustness.** To avoid service failure, WMNs must be robust to link failures or congestion. Routing protocols also should perform load balancing.

3 Routing Metrics

Routing metrics for WMNs have to fulfill four requirements:

1. Ensuring route stability, i.e., no frequent route changes
2. Determined minimum cost/weight paths have good performance
3. Efficient algorithms for calculation of minimum cost/weight paths available
4. Ensuring loop free forwarding

Hop count is the classical routing metric, which is easy to determine. However, it does not give any information about the wireless environment, except that two nodes have a direct link.

Expected Transmission Count (ETX) metric predicts the number of required transmissions for sending a data packet over the link, which includes retransmissions. ETX is calculated from the forward and reverse delivery ratio of a link. It is estimated based on probe packets. It is capable of finding interferences among links.

Per-Hop Packet Pair delivery (PPD) is measured by sending two back – to – back probe packets between the node and its neighbor. It has less impact on queuing delay and other traffic load conditions. It captures the per-link performance parameters.

4 Routing Protocols

The protocols for wireless mesh networks can be basically divided into *proactive, reactive* and *hybrid* approaches. Proactive protocols are more similar to the classical routing strategies such as distance-vector routing. Proactive protocols constantly discover routes and maintain them in routing tables. Hello packets are exchanged periodically by which nodes get informed of changes in the topology. This results in low route discovery latencies at the cost of imposing high overhead due to occupying the bandwidth for route maintenance.

On the other hand, reactive protocols discover and maintain routes only if needed, which results in initial delays until the routes are set up. However, the advantage of this type of routing is low overhead in terms of processing and memory along with minimum power consumption and lower bandwidth requirements. In case of topology changes, which result in link failures, route error messages are generated. Although this will be only done for the routes in use, the problem of imposing traffic at times of topology changes is not solved completely. Ad-Hoc On-Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) are examples of reactive protocols.

To provide more efficiency and scalability, a third group of protocols was introduced as hybrid routing protocols, which is a combination of both reactive and proactive approaches. However, the above mentioned limitations are still in place. An example of a hybrid routing protocol is Zone Routing Protocol (ZRP)..

Another classification of the protocols that depends on the routing metric is:

- Hop Count Based Routing – protocols based the on metrics of the hop-count type. Though these protocols do not in fact indicate the most effective connection paths, they are still in common use due to their low computational complexity.
- Link-Level QoS Routing – this group includes protocols that use the cumulative or the bottleneck value that defines the quality of the connection path
- End-to-End QoS Routing – these protocols are based on the quality parameters, but in a global approach, i.e. for the end-to-end connection path.

- Reliability-Aware Routing – protocols based on the assumption of the availability of a number of simultaneous routes. In this group of protocols, depending of available implementation, packets are sent concurrently along a number of routes, or alternative routes are used only as an auxiliary solution.
- Stability-Aware Routing – protocols grouped in his category use a special architecture of the system to improve the stability of the operation of a network. These protocols prefer cable connection links in MESH networks or links in which no sections (segments) that are executed via mobile users are included.
- Scalable Routing – protocols for large networks where scalability is pivotal. The most typical representatives of this category are the hierarchical and the geographical routing.

5 Security Goals

The unique characteristics of wireless mesh network such as dynamic topology and decentralize nature makes it highly vulnerable to more attacks compared to wired networks. The issues in providing security to WMNs include dynamic topology, physical security of nodes, limited resource availability, open working environment. The various security goals are

Confidentiality: Confidentiality ensures that computer-related assets are accessed only by authorized parties thereby protecting information which is exchanging through a mesh network. It should be protected against any disclosure attack like eavesdropping (i.e., unauthorized reading of message)

Availability: Availability means the resources are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack.

Authentication: Authentication is essentially assurance that participants in communication are authenticated and not impersonators. The recourses of network should be accessed by the authenticated nodes.

Authorization: This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only.

Integrity: Integrity means that assets can be modified only by authorized parties or only in authorized way. Integrity assures that a message being transferred is never corrupted.

Non-repudiation: A node which sends a packet to a destination node cannot later deny that it didn't send the packet and the destination cannot deny receiving the packet.

6 Issues in Network Layer

The attacks in WMNs can be further classified as follows:-

- External Attacks : Attacker can jam the communication in the network. Attacker which is not belonging to mesh network can inject any information in the network. Active attacks can occur at this stage means attacker may can modify and inject the messages into the mesh networks.
- Internal Attacks : These are the most severe attack which can come from compromised nodes inside the mesh networks. Its prevention is not that much easy as compare to external attacks prevention. Passive attacks can be occurred in this type of attacks. Attacker can steal the traffic and inject the messages within the network.

The attacks on network layer in WMNs can be divided into two categories: control plane attacks and data plane attacks. Attacks on control plane targets the routing functionality of the network, while data plane targets the path forwarding functionality of the network.

A. *Data plane attacks*

Data plane attacks are launched by misbehaving nodes in the network. The misbehaving nodes into two groups: selfish and malicious nodes. A selfish node is only concerned about improving its performance even at the expenses of other nodes, while a greedy node intends to disrupt normal network's operation. The simplest data control attack is eavesdropping: Since routing data can reveal information the network topology in general, an attacker by eavesdropping tries to discover this information by listening to network traffic.

B. Control plane Attacks

The main *control plane attacks* are distinguished in:

- *Byzantine attack:* This type of attack may be launched by a single compromised node or by group of working together compromised intermediates. Their goal is to create routing loops and forwarding packets in a long route instead of optimal one, even may drop packets. This attack degrades the routing performance and also disrupts the routing services.
- *Wormhole Attack*: A wormhole attack attempts to convince nodes to use a malicious path through legitimate means. During this attack, two or more malicious nodes collude together by establishing a tunnel, i.e a wormhole, using an efficient communication medium. Once the victim node includes the malicious nodes in the routing path, the malicious nodes start dropping packets.
- *Sinkhole (or blackhole) Attack*: A sinkhole attack is launched when a malicious node convinces neighboring nodes that it is the "most optimal" node for forwarding packets. Then the malicious node drops the packets forwarded by neighboring nodes.
- *Greyhole Attack*: This type of attack is a variant of the sinkhole attack. More specifically, the malicious nodes in contrast to sinkhole attack do not drop all the packets but they just drop selective packets.
- *Routing Attacks*:
  - Location Disclosure: A location disclosure attack reveals information about the location of nodes or about the structure of the network.
  - Rushing Attack: In on-demand routing protocols, the attacker sends a lot of routing request packets across the network in a short interval of time keeping other nodes busy from processing legal routing request packets.
  - Routing Table Overflow: In this attack the attacker attempts to create routes to nonexistent nodes with intention to create enough routes in order to prevent new routes from being created or to overwhelm the protocol implementation.

▪ Route error injection Attack: During this attack, a malicious node injects forged route error messages to break mesh links and disrupt the routing services.

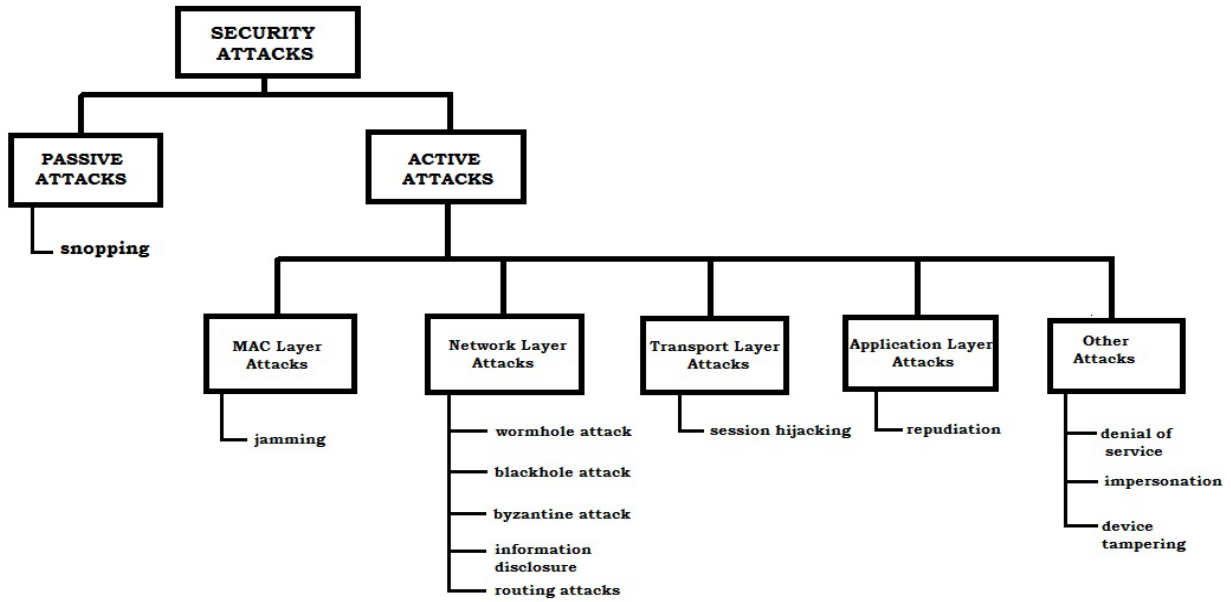

FIG 2. ISSUES IN WMNS

TABLE 1
COMPARISION OF DETECTION METHODS

DETECTION SCHEME	ATTACKS DETECTED	ROUTING PROTOCOL	STANDALONE / COLLUDING	PROS	CONS
BSMR [3]	Byzantine insider attacks	BSMR	Colluding	Software based solution , Can detect colluding attackers	Fails due to larger overhead
CHEMAS [5]	Selective forwarding attacks	-	-	Larger detection rate	Fails due to larger overhead
Sprout [6]	Greyhole and Blackhole Attack	Sprout	Colluding	Capable of detecting large number of colluding attackers	Chooses polluted routing path
MDT [7]	Jamming, Greyhole and Sinkhole attacks	DSR	Standalone	Reliable , high latency of reaching the base station	Collision occurs due to Same packet reaching the base station via different topologies
LEDs [9]	Denial of Service attacks	-	-	Provides various security services	Suffers from larger overhead, maximum usage of network

					resources
UNMASK [15]	Control and Data plane attacks	LSR	2 -4 Colluding Attackers	Light weight scheme also uses LSR , a secure routing protocol.	Not applicable for mobile networks
CAD [17]	Standalone Greyhole Attack.	AODV	Standalone	Capable of Detecting many attacks and High Packet Delivery Ratio.	Inefficient in case of colluding attackers
FADE [21]	Colluding Greyhole attack	AODV , OLSR	Colluding	Capable of detecting colluding attackers and High Packet Delivery Ratio.	Attack detection is difficult when the network size is large

CONCLUSION

WMNs are used for military applications where secure routing of information is the major requirement. This analysis deals with network layer attacks and the different detection techniques adopted. These detection techniques provide feasible result in case of finding the malicious nodes and no suitable scheme is adopted to isolate the malicious node from the network. Hence the future work may include some secure routing principles for isolating the malicious node and rerouting in an efficient way.

ACKNOWLEDGMENT

I would like to thank the authors mentioned in the references which are cited below for their valuable research works which helped me to gain knowledge. And also I thank my guide for her precious guidance.

REFERENCES

[1] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures" Elsvier's Ad Hoc J., vol 1 no. 2-3 pp 293-315 Sept 2003.

[2] F. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Commun. Mag.*, vol. 43, no. 9, pp. S23-S30, Sept. 2005.

[3] R. Curtmola and C. Nita-Rotaru, "BSMR: Byzantine-resilient secure multicast routing in multi-hop wireless networks," in *Proc. Sensor, Meshand Ad Hoc Communications and Networks*, June 2007.

[4] Gao Xiaopeng and Chen wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks" ,IFIP International Conference on Network and Parallel Computing Workshops 2007, pp 209-214, Sept 2007.

[5] B. Xiao, B. Yu, and C. Gao, "CHEMAS: identify suspect nodes in selective forwarding attacks," *J. Parallel and Distrib. Computing*, vol. 67, no. 11, pp. 1218-1230, Nov. 2007.

[6] J. Eriksson,M. Falaotsos, and S.V. Krishnamurthy, "Routing amid colluding Attackers," in Proc. 2007 ICNP, pp. 184-193

[7] H.N. Sun, C. M. CHEN and Y. C. H Asiao, " An efficient countermeasures to the selective forwarding attack in wireless sensor networks " in Proc. 2007 TENCON pp. 1-4.

[8] D. Manikantan Shila and T. Anjali, "Defending selective forwarding attacks in mesh networks," in *Proc. 2008 Electro/Information Technology Conference* , Ames, IA, May 2008.

[9] K. Ren, W. Lou, Y. Jhong : LEDs : providing location aware end-to-end data security in wireless networks" IEEE Trans. Comput. ,vol. 7,no. 5, pp 585-598, 2008.

[10] F. Oliviero and S. P. Romano, "A reputation-based metric for secure routing in wireless mesh networks," in Proc. 2008, GLOBECOM, pp. 1-5.

[11] D. M. Shila and T. Anjali, " A Game Theoretic Approach to gray hole attacks in wireless mesh networks", IEEE International Conference on Military communications 2008, pp. 1-7, Nov 2008

[12] W.Wang, B. Bhargava and M. Linderman, "Defending against collaborative packet drop attacks on manets" in DNCMS2009.

[13] M. Tiwari, K. V. Arya, R. Choudhary and K.S. Choudhary, "Designing intrusion to detect black hole and selective forwarding attacking in WSN based in local information" in Proc. 2009 ICCIT, pp. 824-828.

[14] S. Khan, K.-K. Loo, N. Mast, T. Naeem, " SRPM: Secure Routing protocol for IEEE 802.11 infrastructure based wireless mesh networks," J. Netw. Syst. Manage., vol. 18,no. 2,pp. 190-209, 2010.

[15] Khalil, S. Bagchi, C. N. Rotaru and n. B. Shroff, " Unmask: utilizing neighbour monitoring for attack mitigation in multihop wireless sensor networks" Ad Hoc Netw. Vol 8, no. 2, pp 148-164, 2010.

[16] Sahil Seth, Anil Gankotiya, "Denial of service attacks and detection methods in wireless mesh networks" ITC 2010, pp. 238-240.

[17] D. M. Shila, Y. Cheng, and T. Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in WMN's," IEEE Trans. Wireless Commun.,vol. 9, no. 5, pp. 1661-1675,2011.

[18] V. V. V and V.M. A. Rajan, "Detection of colluding selective forwarding nodes in wireless mesh networks based on channel aware detection algorithm" MES J. Technol. Manage., pp. 62-66, 2011.

[19] Monika, "Denial of Service Attacks in Wireless mesh networks," IJCSIT Vol 3 (3), pp4516-4522, 2012.
[20] Yashpal Rohilla and Preeti Gulia, " A Comparative Study of Wireless Mesh and ad-hoc network : A CrossLayer design approach," IJCSE. Vol. 4,pp. 1181-1184, June 2012.
[21] Quiang Liu, Jianping Yin, Victor C. M.Leung, ZhipingCai, "FADE: Forwarding Assesment Based Detection of collaborative gray hole attacks in WMN's" IEEE Transactions on Wireless Communications, Vol. 12, no. 10, October 2013, pp. 5124-5137.