A Survey of Secure Routing Protocols for Wireless Mesh Networks

Thillaikarasi
Associate Professor
Saranathan College of Engg
Tiruchy-12, Tamil Nadu, India

Mary Saira Bhanu
Associate Professor
National Institute of Technology
Tiruchy-09, Tamil Nadu, India

ABSTRACT

Wireless mesh network (WMN) is the subsequent pace in the development of wireless architecture which provides wireless internet connectivity in an extensive topographical area. Key advantages of WMNs include simple installation, low cost, self-connectivity of nodes, network flexibility and discovery of newly added nodes. WMN is used to integrate different types of networks such as the Internet, cellular, Wi-Fi networks, Wi-Max, sensor networks, etc. The Gateway and bridging functions of the mesh routers enable them to form a hybrid network. In WMN, security is a major challenging issue due to its physical channel vulnerability, dynamic change of the topology etc., which necessitates extensive research to design new security protocols for all layers from physical layer to application layer of the protocol stack. Network layer attacks have paramount significance since they may lead to paralyzing a larger scale network services. The major issue in providing seamless services in WMNs is the design of a secure routing protocol. This paper presents a thorough survey of different secure routing protocols for WMN.

Keywords

Wireless Mesh Networks, Security, Routing Algorithms

1. INTRODUCTION

WMNs encompass of radio nodes organized in a mesh topology and often consist of Mesh Clients (MC) and Mesh Routers (MR). MRs have no or minimal mobility while MCs are static or mobile in nature. The architecture of WMN is classified into Infrastructure WMN, Client WMN and Hybrid WMN. Infrastructure WMN provides backbone for the conventional clients and MCs can communicate via MRs only. In Client WMN, MRs are not required and MCs together form a mesh network with a same radio technique. Hybrid WMN provides interoperability between variety of networks such as Wi-Fi, sensor, Wi-Max and client WMN (see Figure1). WMN supports numerous applications such as broadband home networking, community and neighborhood networking, enterprise networking, building automation, transportation systems, health and medical systems, security surveillance systems, emergency disaster networking and P2P communications [1]. The complexity of network deployment and maintenance is greatly reduced due to its self-organized capacity [4]. For any type of wireless network, security is a major concern due to its physical channel vulnerability, dynamic change of the topology, computational and memory constraints of nodes. Various mechanisms used for providing security in WMN are securing routing and MAC (Message Authentication Protocol) protocols, intrusion detection systems, trust management and key management. The design and implementation of a secured routing or MAC protocols is still a challenging task due to factors like the emergence of new applications that runs on a different environment and the origination of attacks from different layers. This paper discusses various approaches used in providing security at network layer of WMN. The rest of this paper is organized as follows: In section 2 the characteristics of WMNs are summarized. Section 3 discusses various secure routing protocols and their limitations and the paper is concluded in section 4.

2. CHARACTERISTICS OF WMNS

WMN is a multi-hop wireless network that supports ad hoc networking. It has the capability of self-forming, self-healing and self-organizing the network. Mesh routers are capable of providing bridging and gateway functions which lead to the integration of different types of networks. With an advantage of having different architectures, WMN supports different types of network access to the end users. In WMN mobility of the nodes differs (i.e. MR – static and MC- mobile) and hence power consumed by the nodes also differs. Since mesh routers have equipped with multiple radios, transfer of control messages with MRs and data with MCs are possible at the same time. This significantly improves network capacity.

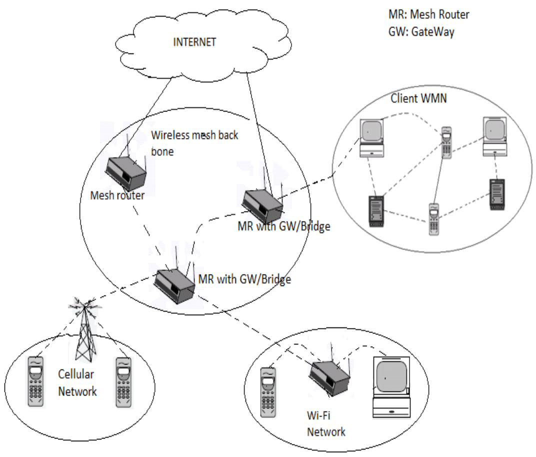

Figure 1: Hybrid Mesh Network

The important factors that are to be considered in the design of WMNs are radio techniques, scalability, mesh connectivity, QoS, ease of use, compatibility, inter-operability and security.

3. SECURING WMNS

3.1 Security attacks

An attack is an attempt to evade security services and violate security policies of the system. WMNs are exposed to common attacks like eavesdropping, traffic analysis, masquerade, replay, denial of service, modification and repudiation. Security attacks can be classified based on their nature, scope, behavior and the layer targeted by the attacker as shown in Figure 2.

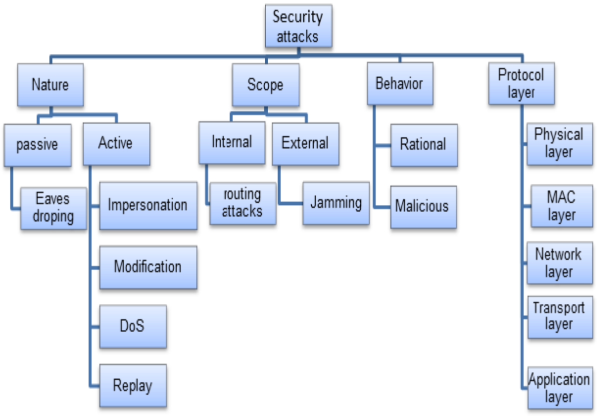

Figure 2: Various types of attacks

Attacks are classified into passive (without any data modification) attacks and active (modification of data) attacks based on the disturbance imposed to the network resources. Eavesdropping and traffic analysis are passive attacks whereas masquerade, modification of messages, replay and repudiation are active attacks. The attack can be classified as internal or external based on the person launching the attack. External attacks are launched by the intruders who are not legitimate users and their aim is to degrade the performance of the network. Denial of Service (DoS) is such a type of attack. Internal attack is launched by the compromised malicious or selfish nodes. The attackers may be categorized as rational attackers (who gains something in terms of quality or price) or malicious attackers depending upon the behavior of the attackers. The attacks might appear in Physical, MAC, Network, Transport and Application layers of the protocol stack.

The attacks on different protocol layers are shown in figure 3. Jamming and eaves dropping attack might occur at Physical, MAC and Network layer. Similarly, flooding and replay attack might occur at Network and TCP layer.

3.2 Security challenges in WMNs

There are several difficulties exist in providing security in WMN [3].

1. Shared wireless link: Since the same radio channel is used by mesh clients to send and receive data packets, attacks like MAC Layer eavesdropping or the replay back are possible.

2. Dearth of association: Due to the ad hoc nature of WMN, the trust relationship among nodes also changes.

3. Physical Vulnerability: Probability of the node being compromised due to the lack of physical protection.

4. Resource Availability: The conventional schemes for achieving security are not appropriate for WMN because of memory and computational constraints.

3.3. Attacks on Network layer

This section presents the various attacks possible on the network layer. The network layer is responsible for transmitting data packets and routing messages. Data packets require end to end security, integrity and authenticity whereas routing messages require hop by hop security services because they are being processed and sometimes modified by the intermediate nodes. Routing protocols should be secure enough because some of the fields in the routing messages are mutable and some are immutable during transmission. Attacks on the network layer are broadly classified into control plane attack and data plane attack as shown in Figure 4.

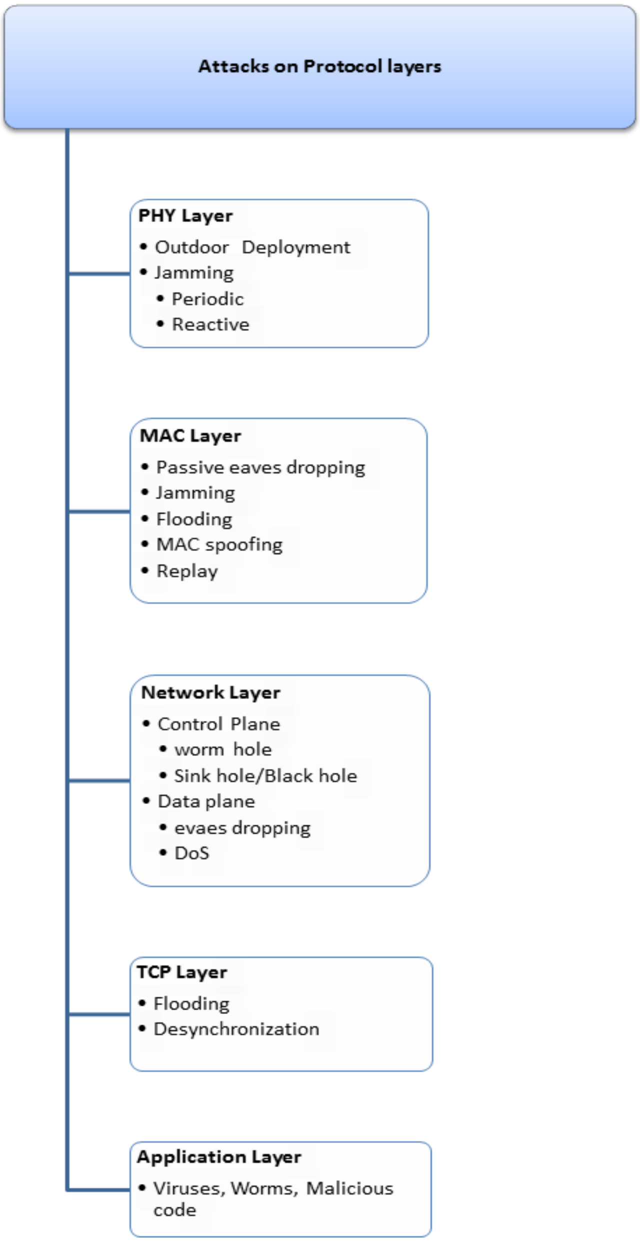

Figure 3: Attacks on different protocol layers

3.3.1 Control plane attack

Control plane attack targets the routing functionality of the router [3].

1) Routing table overflow attacks: An attacker tries to generate false routes and store them in the routing table which prevents the legal nodes to store valid routes.

2) Wormhole Attack: A tunnel is established by two or more malicious nodes and one node captures the packets and tunnels them to another node. The tunnel between two colluding attackers is referred to as a wormhole.

3) Black Hole / sink hole Attack: A malicious node which does not have a valid route is the first one to reply to the Route Request (RREQ) message, so that the packets forwarded through it may be dropped.

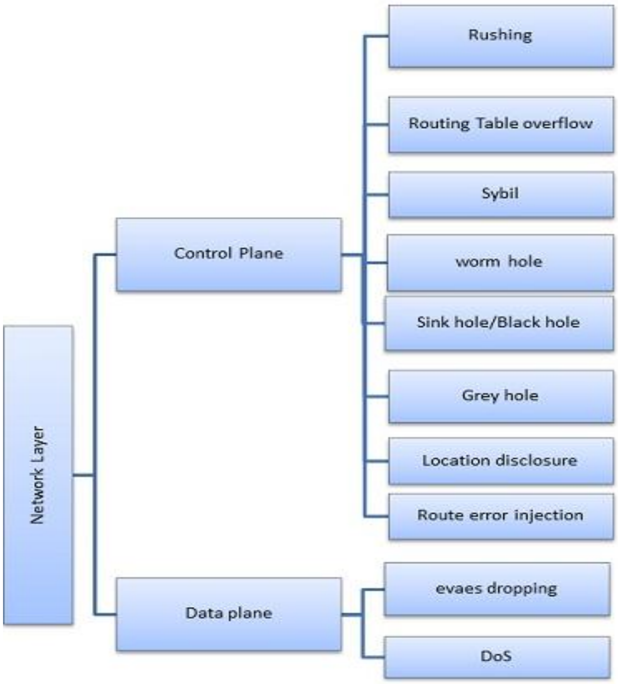

Figure 4: Attacks on Network layer

4) Impersonation attack: If proper authentication mechanisms are not used, compromised nodes may be able to join in the network and send false routing information.
5) Sybil attack: A malicious node may create multiple identities and control network resources.
6) Route reply loop attack: The routing path may loop over some nodes resulting depletion of energy of all participating nodes.
7) Route Request flooding attack: A malicious node tries to flood RREQ messages and leads the poor bandwidth utilization.
8) Route redirection attack: This attack is launched by a malicious node by altering the values of the mutable fields.
9) Network partitioning attack: The network is divided into a number of disconnected partitions by the colluded malicious nodes, which leads to a DoS attack.
10) Rushing attack: A malicious node performing this attack forwards the RREQ packets as soon as any other legitimate node forwards and so it will be a participating node in a path between the source and destination. This attack performs the control plane attack first followed by the data plane attack

3.3.2 Data plane attack

Data plane attack targets the delivery of the data packets. Selfish and compromised nodes may thwart packet forwarding which leads to a DoS attack.
The following strategies are needed to be considered to provide security for WMNs:

i) Security mechanisms should be embedded into routing protocols and MAC protocols
ii) Network monitoring should be developed.

3.4 Secure routing protocols

Various secure routing protocols developed so far can be classified as proactive or reactive (see Figure 5). This section describes some of the well-known protocols such as SRP (Secure Routing Protocol), ARAN (Authenticated Routing Protocol for Ad-Hoc Networks), SEAD (Secure Efficient Distance Vector Routing), SAODV (Secure Ad-Hoc on Demand Distance Vector), and SLSP (Secure Link State Routing).

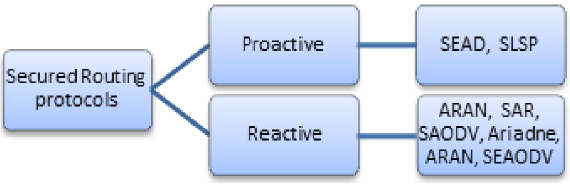
Secured Routing protocols
Proactive
Reactive
SEAD, SLSP
ARAN, SAR, SAODV, Ariadne, ARAN, SEAODV

Figure 5: Classification of secure routing protocols

3.4.1 Proactive Protocols

Proactive or Table driven protocol maintains a routing table at each node and periodically updates it. They are further classified as symmetric, asymmetric and hybrid protocols depending upon the key used to provide security. SEAD is symmetric whereas SLSP is asymmetric in nature.

3.4.1.1 Secure Efficient Distance Vector Routing (SEAD) protocol

Y.-C. Hu et al. proposed a symmetric routing protocol SEAD [10] that is based on Destination Sequenced Distance Vector algorithm (DSDV-SQ). This protocol is designed to overcome DoS and resource consumption attacks. The sequence number is used to overcome long lived rooting loop and replay of routing update message. One way hash function is used to authenticate the sequence number and routing table update messages. It generates hash chain H_0, H_1,….H_n where H_0 is an initial random number generated and the remaining hash chain values are computed as H_j=Hash (H_{j-1}) for $0 \leq j \leq n$, for some value of *n*.

SEAD uses the sequence number i to authenticate the routing table update message as follows.

1. Let m be the upper bound value (i.e. diameter of the network) for the metric distance in the routing table.
2. If H_0, H_1,….H_n is the hash chain of a node and k = (n/m) –i then an element from group of elements H_{km}; H_{km+1}; : : : ; H_{km+m-1} is used to authenticate the routing update message.
3. If j be the metric then H_{km+j} is used to perform authentication.

Whenever a node receives this update, it computes the hash value and if a match occurs it will update its routing table entry otherwise discard it. It is impossible for the malicious user to alter the H_{km+j} value, as $H_{km+j-1}$is needed for alteration. This protocol is used to overcome DoS attacks and resource consumption attacks. The main disadvantage of this protocol is the use of a trusted entity (responsible for symmetric key distribution) which may run into a bottleneck problem during heavy traffic.

3.4.1.2 Secure Link State protocol (SLSP)

SLSP [14] proposed by P. Papadimitratos et al. is an asymmetric protocol and it is based on link state protocol. A secure topology discovery and distribution of link state packets are major goal of this protocol. Every network interface of a node has a pair of keys (private and public key) and one way hash function. Key distribution and management has been taken place in a distributed way using threshold cryptography. The NLP (Neighbor Lookup Protocol) is used to broadcast link state information periodically. It also informs SLSP protocol about suspicious activities like two packets having different IP address but having same MAC address by generating notification messages. Such packets are discarded by SLSP protocols. In addition to this, the hop count field is authenticated using hash chain and link state update (LSU) packets are authenticated by digital signatures which also improve security. When a node receives the LSU packet, it verifies the signature using the public key of the sender. SLSP assigns priority to each node based on their rate of generation of packets. Malicious nodes attempts to flood the network with fake packets which will be always assigned with a lower priority and thus DoS attack is prevented. Further, this protocol is a solution to IP spoofing, MAC spoofing attacks but it is vulnerable to colluding attacks such as wormhole and black hole attacks.

3.4.2 Reactive Protocols

Reactive or on- demand routing protocols discover the route in an on-demand basis by flooding RREQ messages. Reactive protocols are also classified into symmetric, asymmetric and hybrid according to the key used to provide security. In SAR (Security-aware Ad hoc Routing) and SRP (Secure Routing Protocol) confidentiality and authentication can be achieved by symmetric algorithms. Asymmetric algorithms are used by SEAODV, Ariadne, ARAN and hybrid of both symmetric and asymmetric algorithm is used by SAODV protocol.

3.4.2.1 Security-aware Ad hoc Routing (SAR) protocol

According to S. Yi et al. SAR [8] is a symmetric protocol based on on-demand protocols such as AODV or DSR protocol. Unlike other protocols where hop count is used as a metric, SAR uses the security attributes of the nodes to select a secured route between any two nodes to transfer information. If more than one route satisfies the security constraints then the shortest path between them is used for communication. Conversely, if there is no path that satisfies the security constraints then communication cannot take place even though the network is connected. Prior to commence of communication, a trust level of each node is assigned which depends upon the security, significance and capability of the mobile nodes. Trust level assigned to the nodes is immutable and it should be encrypted and appended to RREQ or Route Replay (RREP) messages. All the nodes having same trust level share a secret key and hence they can only be able to decrypt the messages. During the route discovery process the sender node broadcasts a RREQ message with a required security level to establish a new route. The protocol ensures that if the trust level of the intermediate node receiving RREQ is as same as that of the sender, then it can update the security guarantee field in the RREQ (that is used by the sender to set a new route with enhanced security later) and forward the RREQ to its neighbors. If the trust level is different, then the RREQ messages are dropped by the intermediate nodes that cannot provide security. If the routing table at the intermediate node has a route to destination then RREP message is sent by the intermediate node, otherwise destination sends the RREP message. In conclusion, SAR is used to overcome attacks like fabrication, modification, interception and interruption but it is vulnerable to replay attacks, DoS attacks.

3.4.2.2 Secure Routing Protocol (SRP)

SRP proposed by P. Papadimitratos et al., [9] is a protocol based on Dynamic Source Routing (DSR) or Zone Routing Protocol (ZRP). The source node can receive the precise topological information by discarding fabricated route reply messages from the malicious nodes. This protocol assumes a secret key (K_s) between every pair of nodes prior to communication and the nodes are non-colluding nodes. The source node broadcast the RREQ message with the following information

Qseq - Query sequence number,
Qid - query identifier,
IP_s - IP address of source,
IP_d - IP address of destination and
MAC computed for Qseq, Qid, IP_s and IPd.

The neighbor node upon receiving RREQ appends its IP address to the message and broadcasts it. When the Destination node receives the RREQ message, it validates the MAC and sends a RREP message along with MAC back to the source using the route information provided by the RREQ message. The destination may receive one or more RREQ message through different routes and hence it may send more than one RREP message through different routes. The source updates the topological information using the various RREP messages it receives through different paths and acquired the complete knowledge about the network. SRP is specially designed to overcome replay attack. The disadvantage of this protocol is an unauthorized modification of messages by the intermediate nodes.

3.4.2.3 Secure Ad hoc On-demand Distance Vector (SAODV) routing protocol

SAODV [11] protocol is the secured extension of AODV protocol offered by M. G. Zapata et al. This protocol is reactive and hybrid in the sense that it makes use of both symmetric and asymmetric cryptographic algorithms. One way hash function is used to authenticate mutable metric such as hop count and digital signature is used to authenticate immutable metrics of routing messages. The information about the hash functions and digital signatures are transmitted along with RREQ and RREP messages as signature extension. A key management system is needed to distribute public key of the nodes to generate the digital signature. Signature extension field possesses the following information.

a) The hash field contains a random seed.
b) Max_hop count field contains a TTL value.
c) Top_hash contains H (seed, Max_hop count) where H is a hash function and
d) Hash function contains the ID of the hash function used.

When a node receives a RREQ or RREP message, it verifies the hop count value by checking whether Top_hash is equal to H (seed, Max_hop count – hop count). The intermediate node computes Hash = H (Hash) and update the hash field before rebroadcasting the message. Integrity of immutable fields of RREQ and RREP messages are preserved using digital signatures. After receiving the RREQ message, AODV allows the intermediate node (having a route to the destination in its route table) to send RREP to the source on behalf of the destination node. The signature is verified by SAODV using either of two extension messages i.e. RREQ and RREP with Double Extension Signature or Single Extension Signature. In Single Signature Extension method, intermediate node is not allowed to send the RREP message back to the originator. Destination node alone is responsible to send to a RREQ message. In the case of Double Extension Signature method the intermediate node may reply to a RREQ message. RERR (Route Error) message is also signed and verified in a hop by hop manner. The computational overheads due to asymmetric cryptographic algorithms are more when compared to other protocols.

3.4.2.4 A secure on-demand routing protocol for ad hoc networks (ARIADNE)

Y.-C. Hu, et al. proposed secured version of DSR protocol named Ariadne [12]. TESLA, an efficient broadcast authentication protocol is also used for authenticating the routing message. Three different authentication mechanisms are used by this protocol, each relying on different keys and different distribution mechanisms.

- Pair wise shared key: If n is the total number of links in the network then n*2 keys (i.e different keys for each direction) are used for providing confidentiality and authenticity. They are distributed using Key Distribution Center (KDC).
- Digital signature: Each node generates their own public and private key pair and the public keys are distributed either using KDC or using the certified authority.
- TESLA: Assume all nodes have pair wise secret keys to generate MAC and a public key per node to generate one way key chain and these keys are distributed among all the nodes. Time synchronization between nodes is a major constraint for this protocol. Each node computes one way key chain as follows:

  If PU_a is a public key then $K_n=PU_a$,
  K_{n-1} = Hash (K_n),……… K_i = Hash (K_{i+1}), …. K_1, K_0 = Hash (K_1).

Each node discloses its key K_i at a time t_0+i*j where t_0 is K_0's disclosure time and j is the publication time interval for the key and the keys are published in reverse order (i.e. K_0, K_1, ….K_n). During route discovery process source node computes MAC (hash chain value) using the key K_{ST} (secret key shared between source and target),appends this to the RREQ message which contains the source address, target address, id for the request message, expected time to reach destination, key list and MAC list and broadcast it. Consequently, a neighbor node receiving this request computes new hash chain value, MAC value using its TESLA key and rebroadcast the modified RREQ message if the time interval is valid. Otherwise, the packet is discarded. Each node in the route from source to destination appends their address and MAC computed using the TESLA key in the RREQ message. A destination node after verifying the hash chain value generates a MAC using key K_{TS} (secret key shared between the target and source), appends MAC and empty key list to the RREP message and forwards the message back to source along the reverse path stated in the node's list. On receiving this RREP message the intermediate nodes wait until the time interval expires and discloses its TESLA key to the key list. When the source node receives the RREP message it validates each key in the key list, verify the authenticity of the MAC generated using key K_{TS} and each MAC in the MAC list. If the validation phase is successful then, RREP is accepted by source node, otherwise it is discarded. Similarly, whenever a node not able to forward the packet to its next hop (due to link failure); it will send a RERR message back to the originator. The drawbacks of this protocol are time synchronization and delayed verification & validation of keys.

3.4.2.5 Authenticated Routing for Ad hoc Networks (ARAN) protocol

ARAN [13], a reactive asymmetric protocol proposed by K. Sanzgiri et al. is responsible for end to end route authentication, message integrity and non-repudiation. A centralized certificate authority is responsible to issue the certificates for legitimate users and its public key is known to all legitimate users in prior. Whenever a node registers itself in a network, it receives a certificate from the authority. The certificate encompasses IP address and public key of the node, time of generation and expiration time of the certificate. The RREQ message encrypted with source's private key contains a timestamp, nonce, packet identifier, IP address of the destination and certificate of source. Any intermediate node receiving the RREQ packet after verifying the certificate of its neighbor, append its certificate and encrypt the whole packet with its private key and then forwards it. A destination node after receiving the packet validates source node's certificate, nonce, timestamp values and replies positively with a RREP message. The RREP message uses the reverse path to reach the source and source validates the RREP packet. In case of any mismatch in the nonce and time stamp pair or if certificate fails an RERR message is generated. ARAN protocol is used to overcome passive attacks such as the intrusion of unauthorized node, modification of routing messages and replay attacks. It is vulnerable to DoS attacks, Location disclosure, black hole, wormhole attacks and Route request flooding attack.

3.4.2.6 Security enhanced AODV (SEAODV) protocol

SEAODV [15] protocol proposed by C. Liet, et al. uses Pair wise Transient Key (PTK) and Group Transient Key (GTK) to preserve data integrity and authentication in a hop by hop basis for unicasting and broadcasting the routing messages respectively. PTK is distributed using Blom's key distribution mechanism and GTK is distributed using pre distributed PTK. The MAC is computed for the whole RREQ or RREP message and appended to the message. Whenever the node broadcast or rebroadcast the RREQ message it computes the MAC using GTK (key shared between the node and all of its one hop neighbors). The receiving nodes verify the MAC, modify the hop count field, compute the MAC for the modified message and then rebroadcast it. The intermediate or the destination node may unicast a RREP message and computes MAC using PTK (secret key shared between a pair of nodes).SEAODV overcomes rushing attack and it is vulnerable to RREQ flooding attack. The damage caused by this attack is minimized as it is detected at the early stage of the attack.

4. ANALYSIS OF SECURE ROUTING PROTOCOLS

A comparative analysis of all the above routing protocols is given in the table 1.

Table 1: Comparative analysis of secure routing protocols

S.No	Security Protocol	Proactive or Reactive	Salient features	Metrics	prevention to attacks	Vulnerable to attacks
1.	SEAD [10]	Proactive & Symmetric	• Based on DSDV-SQ protocol • One way hash function • Trusted third party and Clock synchronization of nodes • Hop by hop authentication.	Sequence number & Source of route update message are authenticated.	DoS attack, Resource consumption attacks, Rushing attack.	Location disclosure, black hole, wormhole attacks
2.	SLSP [14]	Proactive & Asymmetric	• Public keys are certified by a trusted third party • Key management using threshold cryptography • NLP is used	Path length	DoS attacks and spoofing attacks.	Location disclosure, black hole, wormhole attacks
3.	SAR [8]	Reactive & symmetric	• Extension of AODV or DSR • Security attributes are needed to define routing metric • Different keys are used to provide different levels of security which leads to the storage and computational overhead	Trust values	Black hole, Rushing attack, Routing table modification attack	DoS attacks, Location disclosure, wormhole attacks
4.	SRP [9]	Reactive &symmetric	• Based on DSR, Security association between end nodes is needed in prior • RREQ and RREP messages are authenticated using MAC • Existence of Non colluding nodes & Intermediate nodes are not allowed to send RREP messages - assumption	Path length	Replay , DoS , Routing table poisoning attacks, Rushing attack, Location disclosure,	Black hole attacks, wormhole attacks
5.	SAODV [11]	Reactive & Hybrid	• Extension of AODV • To secure the routing messages digital signatures and one way hash functions are used • The communication overhead increases as mobility increases	Path length	Replay , Routing table poisoning attacks, Rushing attack, Route reply loop attack	DOS attacks, Location disclosure, black hole, wormhole attacks
6.	ARIADNE [12]	Reactive & Symmetric	• Clock synchronization of nodes • Shared secret key between nodes • End to end authentication • Need for key distribution center	Path length	Replay , DoS , Routing table poisoning attacks, Rushing attack, Selective packet dropping	Location disclosure, black hole, wormhole attacks
7.	ARAN [13]	Reactive & Asymmetric	• Trusted certificate authority is needed • The security associations between nodes are needed in	No specific metric	Unauthorized participation of nodes, Spoofed routing packets, Rushing attack.	DOS attacks, Location disclosure, black hole, wormhole attacks, Route request

			prior			flooding attack
8.	SEAODV [15]	Reactive & Asymmetric	- Extension of AODV - Bloom's key pre distribution scheme is used - Hop by hop message authentication	Path length	Rushing attack, Flooding attack	DOS attacks, Location disclosure, black hole, wormhole attacks

Rakesh Matam, et al, proved that the existing protocols are insecure by using formal verification methods. They have proved that SAODV, SRP, ARAN and Ariadne protocols are prone to attacks like Metric Manipulation Attack, Route Corruption Attack, Routing Loop Attack which is specified in the following table 2 [16].

Table 2: Robustness of existing protocols Protocol

Attacks	SAODV	SRP	ARAN	Ariadne
Metric Manipulation Attack	Yes	Yes	No	No
Route Corruption Attack	Yes	Yes	Yes	Yes
Routing Loop Attack	Yes	No	Yes	No

The following Figure 5 explains the victims that are susceptible to most prevailing attacks like routing table poisoning, wormhole, blackhole, location disclosure, rushing and DoS.

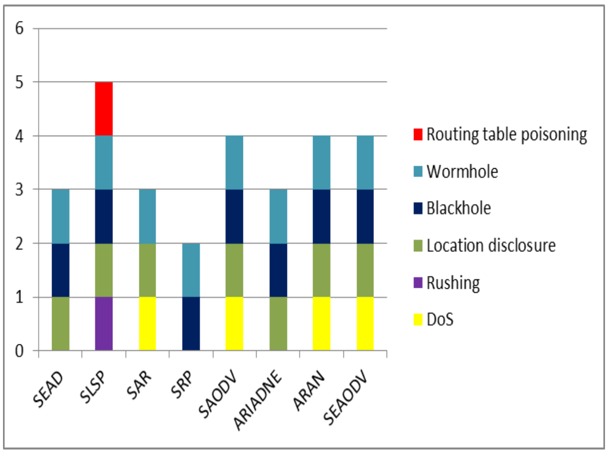

Figure 5: Victims for different type of attacks

From the above figure it can be inferred that SLSP is prone to all type of attacks, rather SRP protocol can restrain most of the above mentioned threats but intractable to Blackhole and Wormhole. Variants of AODV are influenced by the same type of threats.

5. CONCLUSION

WMNs can capable of providing uninterrupted connectivity due to their self-healing nature. The successful secured implementation of WMNs requires traditional and enhanced security protocols. In summary, security attacks, secure routing protocols and their vulnerabilities are presented. The protocols can be proactive or reactive, they can use symmetric or asymmetric cryptographic algorithms and they can use either hop by hop or end to end authentication. SAODV, SEAODV and SAR are an extension of AODV protocol. Most of the protocols made an assumption that the secret keys are distributed securely between the nodes before communication. Some protocols such as SLSP and ARAN assume the presence of trusted certificate authority. Thwarting all security attacks at the network layer and maintaining security is impossible for all the above protocols. This survey proclaims that novel protocols are to be explored to build secured WMNs. Security protocols proposed so far are not solutions for diverse types of attacks launched at different layers. The Security attacks on network layer may due to the events caused at lower layers. Thus a cross layer approach is required to secure WMNs.

6. REFERENCES

[1] Xiang Xu, Xianjie Wu, Zhi Yu. 2010. Application of Wireless Mesh Network in Campus Network. Second International Conference on Communication systems Networks and applications. pp.245-247.

[2] Amandeep Jindal, Anil Gankotiya, Sahil Seth. 2010. A Comparative Study between Wireless Local Area Networks and Wireless Mesh Networks. Second International Conference on Computer Engineering and Applications. vol. 1, pp. 192-196.

[3] Anil Kumar Gankotiya1, Gurdit Sing, SahilSeth2. Attacks and their Counter Measures in Wireless Mesh Networks. Available: http://www.csjournals.com/IJITKM/Special.

[4] Akyildiz, IF, Wang, X and W. Wang. (2005, March). Wireless Mesh Network: A Survey. In Computer Networks and ISDN Systems. Volume 47(4). pp. 445-487.

[5] C. Perkins, E. Belding-Royer and S. Das. (2003 July). Ad hoc On demand Distance Vector (AODV) Routing. IETF RFC 3561.

[6] E Cizeron, J.P. Guédon, S. Hamma and H. Issaka. (2006 Oct). Performance Evaluation of Reactive and Proactive Routing Protocol in IEEE 802.11 Ad hoc Network. In the proceedings of SPIE Next-Generation Communication and Sensor Networks, Volume 6387,

[7] J. Broch, D. A. Maltz, D. B. Johnson, Y-C. Hu, and

J.Jetcheva.(1998 Oct). A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. In the proceedings of the Fourth Annual International Conference on Mobile Computing and Networking (MobiCom'98). pp: 85-97.

[8] Yi, S, Naldurg, P and Kravets, R, (2001). Security-aware ad hoc routing for wireless networks. Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'01), Long Beach, CL, USA, (299 – 302).

[9] P. Papadimitratos and Z. J. Haas. (2002 Jan). Secure routing for mobile ad hoc networks. In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS'02), San Antonio, TX, USA, pp. 27-31.

[10] Y.-C. Hu, D.B. Johnson, and A. Perrig. (2002 June). SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. In Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), Callicoon, NY, USA, pp. 3 – 13.

[11] M. G. Zapata and N. Asokan. (2002 Sep). Securing ad hoc routing protocols. In Proceedings of the 1st ACM Workshop on Wireless Security (WiSe'02), Atlanta, GA, USA, pp. 1-10.

[12] Y.-C. Hu, A, Perrig, and D. Johnson. (2002 Sep). Ariadne: a secure on-demand routing protocol for adhoc networks. In Proceedings of ACM Annual International Conference on Mobile Computing (MobiCom'02), pp. 21 – 38, Atlanta, GA, USA.

[13] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer. (2002 Nov). A secure routing protocol for ad hoc networks. In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02), Paris, France, pp. 78 – 87.

[14] P. Papadimitratos and Z. J. Hass. 2003. Secure link state routing for mobile ad hoc networks. In Proceedings of the Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), pp.379-383, Washington DC, USA,

[15] C. Li, Z. Wang, and C. Yang. (2011 Sep). Secure routing for wireless mesh networks. International Journal of Network Security, vol 13, no 2, pp. 109-120,

[16] Rakesh Matam and Somanath Tripathy. (2014 May). Provably Secure Routing Protocol for Wireless Mesh Networks. International Journal of Network Security, vol 16(3), pp. 168-178.