DIFFERENT SECURITY MECHANISMS FOR DIFFERENT TYPE OF SECURITY LAPSES IN WMN- A REVIEW

Narender Singh

Deptt. Of CSE, Shaheed Bhagat Singh college of Engg. & Tech. , Ferozepur(Punjab)
narenderyadv@gmail.com

Kuldeep Vats

Deptt. Of CSE, Shaheed Bhagat Singh college of Engg. & Tech. , Ferozepur(Punjab)
kuldeepvats@yahoo.com

Jasvinder

Deptt. Of CSE, Shaheed Bhagat Singh college of Engg. & Tech. , Ferozepur(Punjab)
jasrohila@gmail.com

Lovish Jaiswal

Deptt. Of ECE, Shaheed Bhagat Singh college of Engg. & Tech. , Ferozepur(Punjab)
er.lovish39@gmail.com

Abstract

The wireless mesh network(WMN) is a wide network over globe . It is a multi-hop network which is made of static as well as the Mobile nodes which are connected with each other via special node called routers and Backbone gateways. As the infrastructure of WMN is large and it is multi-hop . It is difficult to provide security easily at different communications links. WMN is made up of many type communication media such as wired such as co-axial cable to optical fiber and Wireless Media such as low length WI-FI to high range and capacity Wimax. So it is heterogonous in nature. Due to heterogeneity, security lapses are much more over WMN. There my be several type of attacks which affects the data unlawfully. There are many security mechanisms are deployed which according to transmission media provide adequate security and make WMN a safe network for data transmission. We discussed threats and there possible solution using security mechanisms This paper serves a baseline for developing a secured, full-proof WMN which takes care of all types of attacks.

Keywords : WMN, Security threats, MPLS, VRF BGP,, VPN, IPSec, SSL

1. Introduction

Wireless mesh network is a open network which is made of different type of mobile as well as static nodes. Wireless mesh network(WMN) is made to cover large space over earth. It provide fast internet services at low cost. It is mainly multi-hops network which connect nodes to each other[1]. Nodes as told before as mobile as well as static are of two type. 1) End nodes called clients nodes which are mainly mobile phones ,laptops ,PCs, or some communication device. These are the end nodes having auto-configuration capability to the network. 2) Another's are the routers which connects clients and route traffic from one node to another some routers works as a node to carry traffic from the end nodes(clients) while another are called gateway which pass traffic from simple routers[1].

WMN provides cheap way to access the internet. But this cheapness cause security lapses which make it unsecure mean to communicate over the network. As network is so much large , it is not easy to provide security solution to secure mesh network . It is a multi-hop network spread over large area makes it difficult to apply security over different or each hops[2].

Over the network , there are many type of clients which may send sensitive data, error sensitive data, or may be real time data which is required to send without any security lapse. So WMN is required to secure at every hops not as a whole to save from any type of interruption

2. Security Lapses

There are many type of attacks such as:-

I. Spoofing of wireless network
II. DNS spoofing
III. Blackhole Attack
IV. Wormhole Attack
V. Theft of Service Attack
VI. Location Disclosure Attack
VII. False Message Attack
VIII. Forging
IX. Resource Depletion Attack
X. Route Table And table Overflow
XI. Denial of Services
XII. Signal Jamming[2,19]

These attacks by intruder cause interruption in proper communication between two parties. These attacks may change the data contents which affects integrity of sensitive data or these may cause delay on denies real-time data which cause data unuseful. There are many mechanisms which helps in proper delivery of data. This can be achieved by authentication, encryption, by certification or some secure medium such as VPN , secure protocols IPSec ,MPLS or by combination of two protocols as MPLS-VPN etc.

protocols layers may be attacked such as

Layers	Threats
Application	False Authentication
Transport	Traffic Attacks, Spoofing
Network	Blackhole, Wormhole Denial of Services
Data link	Signal Jamming, Unwanted Packets Flood
Physical	Collision , Contention Battery Exhaust, Traffic Analysis [2,19]

3. Security mechanism

3.1 *MPLS-TE*

MPLS-TE is a traffic engineering approach which provide fast and secure data traffic over the network . It works with the combination of MPLS(multi-protocol label switching) and added security with TE(traffic Engineering). MPLS add label with the packets at Network layer at packet header which help in sending /routing the packets fastly. Label switched Router(LSR) are special router are used to route packets over the network.[2] MPLS-TE provide help to Internet service providers(ISP) to solve problem of congestion in which it enable the data packets from congested path to less congested path or less loaded path[3]. MPLS encapsulated data provide link layer authentication which help from many active attacks in WMN at such as wormhole, Blackhole. It also provides security from spoofing in which intruder change IP address and access data unlawfully. Using MPLS tag technique DNS spoofing is discouraged. Signal jamming and message distortion is also blocked and provide security from such attacks. [2]Data integrity is also remains over the WMN, as tag is only removed at destination node ‘s MPLS device. So data is encapsulated and save from such active attacks.

MPLS-TE provide security in case of flooding attacks. During flooding attack, it recalculate fastly a new secure path [2,6,7].

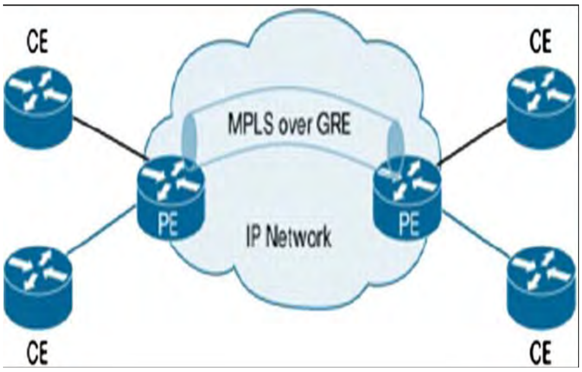

Fig.1 MPLS mechanism of secure Tunnel (CISCO)[2]

MPLS-TE automatically set a secure tunnel[fig.1] between two nodes. Tunnel is made over less cognate path automatically when due to flooding network bandwidth become less available , then it automatically configure new secure tunnel. WMN backbone resources are flooded via extensions to a secure path[2]. MPLS can use different distribution label framework. Present protocols for label distribution include: Resource Reservation Protocol (RSVP), Label Distribution Protocol (LDP) and Border Gateway Protocol (BGP).

3.2. ***Access Control***

WMN use some access control mechanism from older wireless network such as 802.11 , Ad-hoc network, MANET . But one problem is that WMN is a multi-hop network which makes it difficult to applied secure access control over different transmission media. But some security mechanism such as AAA(Authentication, Authorization, Accounting) can be implemented at WMN[2]. In AAA mechanism, there is central server which provide a secure mechanism for communicating parties. It saves from unauthorized node to access data of another trusted node. AAA server manage the secure mean of communication between trusted node[4]. There is a convenient method based on distribution.[fig.2] This method is called Polynomial Distribution Method which is used to distribute key between two trusted parties

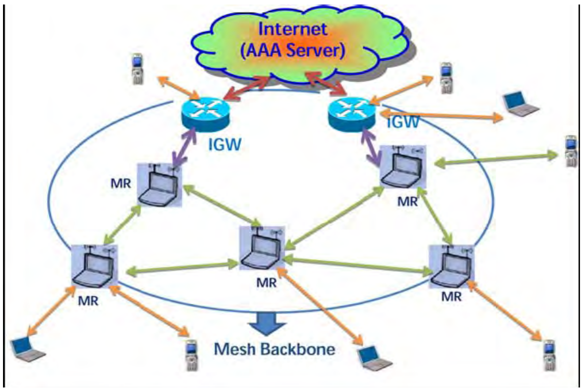

Fig. 2 Access Control in WMN using AAA server [2].

AAA server first distributed the set of secrets over the network entities, then it send some polynomial function to the entities. The entities then individual calculate a secrete key called symmetric key. With that key all the communication is done .

3.3. ***Certification***

WMN is a vast network . Due to multi-hop network ,it is more vulnerable to threat by unautherorised node in WMN. To authenticate the nodes over mesh network ,it is required to certify it by a certificate authority(CA) . But this type of approach is possible in Ad-hoc , MANET, a small private wireless network. For a WMN central type of CA is not works as WMN is a auto-configure network. There is a distributed type of network is required which auto –certify the authentication of clients [5]. There are two type of certification 1) Public key cryptography 2) symmetric key cryptography. There may be possible more than one internet service providers(ISPs) and every operator has its own certification. The operators which decide to cooperate (O1 and O2) issue cross-certificates of their CAs which means that operator O1 issues a certificate on the public key of O2’s CA and O2 issues a certificate on public key of O1’s CA. With the cross-certificates, entities (subscribers or access points) can perform certificate based authentication and key exchange mechanisms even if they belong to different operators [6].

In WMN , there is a certification authority like MANET, Ad-hoc network where certification authority are MOCA [5,23*] and SEKM[5,22*]. Called mesh certification Authority(MeCA). In this certification authority there are n mesh routers(MRs) which are share holders in CA. All n MRs distributes the secret information among all share holder. There are ‘m ‘ MRs among ‘n’ MRs (m<n) which has special authority to change the secret key as well as the functions periodically as keys are sensitive to threat. If a unauthorized node as a fake shareholder see the data, then it will no longer use that information .

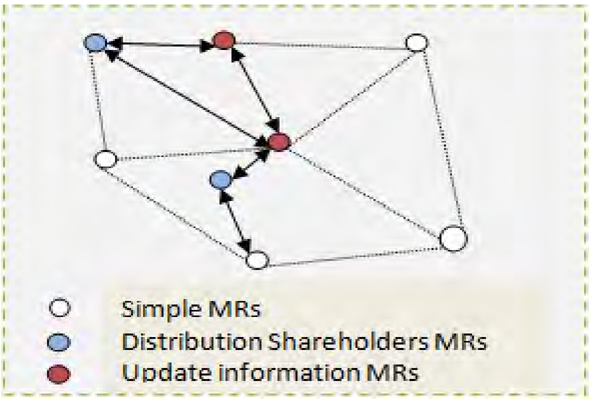

Fig.3 . tree path for secret share distribution in WMN

MeCA certification is done by two steps:-

I. Fast verifiable secret redistribution(FVSR) scheme in which multiple MRs (n) participates in CA distribution. These participants distribute secret information among different participants. Each participants MRs send information to its another participants using a multicast tree. MeCA use multicast in four cases.

1. When secret shares are updated.
2. When the certification revocation message are transmitted
3. When the MeCA function are transfer to other nodes .
4. When MAPs request certification update or status verification [5].

II. Secret Sharing was invented by Shamir[5,24] and Blakley [5,25]. Secret sharing scheme is used to verify the shareholder that they are right shareholder. In WMN verifiable secret sharing(VSS) scheme. In VSS scheme, the dealer broadcasts a zero –knowledge proof for the shareholders. So, to save from authorized attack which gather secret share, share are periodically updated [5].

3.4. *MPLS-VPN*

MPLS-VPN is a family of methods for harnessing the power of Multiprotocol Label Switching (MPLS) to create virtual private networks (VPNs). MPLS is well suited to the task as it provides traffic isolation and differentiation without substantial overhead and security from many threats such as Denial of services(DDoS), spoofing, integrity[2,8,26]. It combine the intelligence of multi-path routing with the layer 2 switching providing added advantage to the IP and other technologies. One of the best thing over simple MPLS is that it added encryption security technique and take advantage of VPN with multi channel assignment which provided security from Dos attack. In WMN , the demand of client may vary so traffic change over the network so it is required to auto-configured the channel assignment so that data will route fastly without any congestion by reconfiguring the network channel assignment [2].

It can be done by many models, one is Global sequential redesign model which help in auto configure the links . This approach allows each failure state to be solved independently, and the capacity requirements for each of the links then can be compared to the maximum requirements for all of the previous solutions. This process may be repeated through all of the failure states, and the final design will represent the capacity needed in each link to carry the maximum flows that result from either the initial state or any of the failure states over all links. We then impose a failure state and redesign the network, using only those links that are not involved in the failure. This process is then repeated for each failure state. After each failure redesign, the capacity requirements for each link are tested. The capacity requirement is set to the larger of the bandwidth requirements for the current failure state and the previous largest requirements for that link. Once all failure states have been tested, the final link capacities will support the bandwidth requirements of any single element failure state [9] so at last there will be no link failure. So it prevents from attacks like flooding.

MPLS-VPN shares the same address space with other wireless networks without interfering network devices such as the MPLS core network and VPN. Furthermore, the data traffic from each VPN remains separate, never accessing other VPN domains. VPN assigns and enables virtual routing and forwarding (VRF) commands and the edge router maintains a separate VRF for each VPN connection and this enhances security of the traffics and data [2,6].

Another advantage of MPLS-VPN is concealment. In it virtual channel is separated over channel and configure automatically so it conceal the actual path of data over the network from intruder and so DDoS threats. [2]

In MPLS-VPN, packets are securely routes using MPLS label signaling and Border Gateway protocol(BGP) which makes routing decisions based on path, network policies and/or rule sets. In WMN packets are passed through secure tunnel using MPLS labeling and BGP provide a path to destination [6,27,28]. Enterprise VPN routes are communicated from the CE to the PE using an Interior Gateway Protocol (IGP) such as the Open Shortest Path Protocol (OSPF) or an Exterior Gateway Protocol such as Exterior Border Gateway Protocol (eBGP) [7].

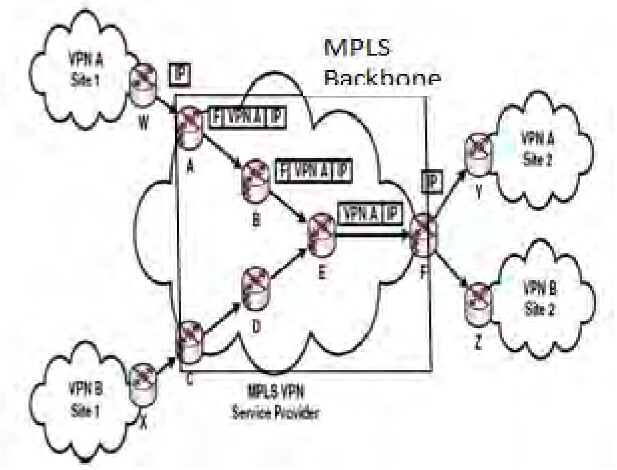

Fig.4 VPN packets through MPLS core with IP

Routing in WMN using MPLS-VPN is done in distributed manner. When route information starts from site1 through secure tunnel over WMN It passes from Customer Edge(CE) router to Provider Edge(PE) routers When a PE router receives a route from a CE router (which it places in the corresponding Virtual routing/Forwarding(VRF) table), it assigns the BGP community specified by the PE.s local configuration to the route, and exports the route to its BGP table [10,29]. The route is then distributed to other PEs using BGP. Each PE router, upon checking its local configuration, then imports this route to VRF tables belonging to the same BGP community. By this complete routing is done and sites can communicate through this path [6,30].

Another advantage of MPLS-VPN is that it provide different VPN channel and each VPN has its own VRF table at each PE router so when packets comes at PE router , it automatically assign correct VPN channel according to its interface according to source and destination address [10]. So it prevent from unauthorized attacker to send data to a client node. Customer VPNs are also separated from service provider networks. Each incoming packet at a PE router is immediately assigned to a VPN and sent to an LER where it is forwarded to a CE router. Consequently, it is difficult to reach an internal router from outside the service providers network [6,31].

3.5. *MPLS-VPN-IPSec*

MPLS-VPN send data traffic over the network using simple Internet Protocol IP. In it ,there is data is sent over optimal route using BGP at PE routers. If IP security protocol IPSec is added with MPLS-VPN feature. This addition provide security by IPSec feature like Authentication, privacy and data protection between peer clients in WMN [2,10,32,26].

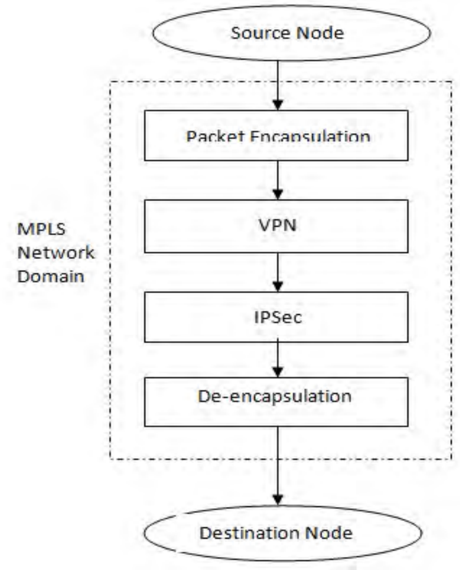

Fig.5 MPLS-VPN-IPSec Security mechanism

So the combination of VPN , MPLS routes the packets using secure IP which provide authentication and quality of services(QoS) in WMN [10]. Actually, IPSec protocol uses two protocols to provide security to data.

I. *Encapsulated Security Payload ESP)*, protects the IP packet data from third party interference, by encrypting the contents using symmetric cryptography algorithms (like Blowfish, 3DES).

II. *Authentication Header (AH)*, protects the IP packet header from third party interference and spoofing, by computing a cryptographic checksum and hashing the IP packet header fields with a secure hashing function. This is then followed by an additional header that contains the hash, to allow the information in the packet to be authenticated [13]. AH operates directly on top of IP, using IP protocol number 51[15,18]. Authentication Headers(AH) provide connectionless integrity and data origin authentication for IP datagram and provides protection against replay attacks [16,17].

IPSec can either be used to directly encrypt the traffic between two hosts (known as *Transport Mode*); or to build “virtual tunnels” between two subnets, which could be used for secure communication between two corporate networks (known as *Tunnel Mode or VPN*) [11,12,13]. But direct encrypt the traffic in IPSec provide less security from attacks while using VPN, it provide security from most difficult solution attack DoS. So with VPN tunnels between two nodes , IPSec provide extra security with above protocols. It is important to understand that VPNs do not remove all risk from networking. While VPNs can greatly reduce risk, particularly for communications that occur over public networks or in WMN, they cannot eliminate all risk for such communications. One potential problem is the strength of the implementation. For example, flaws in an encryption algorithm or the software implementing the algorithm could allow attackers to decrypt intercepted traffic; random number generators that do not produce sufficiently random values could provide additional attack possibilities. Another issue is encryption key disclosure; an attacker who discovers a key could not only decrypt traffic, but potentially also pose as a legitimate user. Another area of risk involves availability. A common model for information assurance is based on the concepts of confidentiality, integrity, and availability. Although VPNs are designed to support confidentiality and integrity, they generally do not improve availability, the ability for authorized users to access systems as needed. In fact, many VPN implementations actually tend to decrease availability somewhat because they add more components and services to the existing WMN infrastructure[2,11]. This is highly dependent upon the chosen VPN architecture model and the details of the implementation. The following sections describe each of the three primary VPN architectures: host-to-host, host-to-gateway, and gateway-to-gateway.

a. Gateway-to-Gateway

IPSec-based VPNs are often used to provide secure network communications between two networks. This is typically done by deploying a VPN gateway onto each network and establishing a VPN connection between the two gateways. Traffic between the two networks that needs to be secured passes within the established VPN connection between the two VPN gateways. The VPN gateway may be a dedicated device that only performs VPN functions, or it may be part of another network device, such as a firewall or router. To facilitate VPN connections, one of the VPN gateways issues a request to the other to establish an IPSec connection. The two VPN gateways exchange information with each other and create an IPSec connection. Routing on each network is configured so that as hosts on one network need to communicate with hosts on the other network, their network traffic is automatically routed through the IPSec connection, protecting it appropriately. A single IPSec connection establishing a tunnel between the gateways can support all communications between the two networks, or multiple IPSec connections can each protect different types or classes of traffic in complete WMN [12,13,14].

b. Host-to-Gateway

An increasingly common VPN model is the host-to-gateway model, which is most often used to provide secure remote access. The organization deploys a VPN gateway onto their network; each remote access user then establishes a VPN connection between the local computer (host) and the VPN gateway in WMN. As with the gateway-to-gateway model, the VPN gateway may be a dedicated device or part of another network device. It provides a protected connection for the remote user [13]. In this model, IPSec connections are created as needed for each individual VPN user. Remote users. hosts have been configured to act as IPSec clients with the organization's IPSec gateway. When a remote user in WMN wishes to use computing resources through the VPN, the host initiates communications with the VPN gateway. The user is typically asked by the VPN gateway to authenticate before the connection can be established. The VPN gateway can perform the authentication itself or consult a dedicated authentication server. The client and gateway exchange information, and the IPSec connection is established. The user can now use the organization's computing resources, and the network traffic between the users host and the VPN gateway will be protected by the IPSec connection. [12,13,14].

c. Host-to-Host

The least commonly used VPN architecture is the host-to-host model, which is typically used for special purpose needs, such as system administrators performing remote management of a single server. In this case, the organization configures the server to provide VPN services and the system administrators. hosts to act as VPN clients. The system administrators use the VPN client when needed to establish encrypted connections to the remote server. the host-to-host VPN is the only model that provides protection for data throughout its transit. This can be a problem, because network-based firewalls, intrusion detection systems, and other devices cannot be placed to inspect the decrypted data, which effectively circumvents certain layers of security. The host-to-host model is most often used when a small number of trusted users need to use or administer a remote system that requires the use of insecure protocols (e.g., a legacy system) and can be updated to provide VPN services [13]

To provide complete security from source node to destination node and over routers and gateways, we need to apply all these models in WMN. VPN-IPSec naturally offers a high degree of data privacy through establishment of trust points between communicating devices, and data encryption with the Data Encryption Standard (DES) or Advanced Encryption Standard (AES) standard. IPSec are used to encrypt the WMN using WAN, IP VPN, or the Internet for connectivity. VPN-IPSec can be deployed across essentially any IP transport, including traditional WAN (such as FR, ATM), IP VPN, and Internet, integrated security services such as firewall can be applied in the WMN. Intrusion Prevention System (IPS) and DDoS prevention systems are resolved within the integrated VPN-IPSec design and it is more frequent at the node peripherals. At IPSec head end locations, security functions have historically been distributed or dedicated devices. We deploy mesh routers and client nodes-acceleration for IPSec to minimize router-tables updates overhead, to support traffic with low-latency/jitter requirements, and for the best performance for overhead. Digital certificates/PKI are used for scalable tunnel authentication. We can also set up QoS service policies, as appropriate, on head end and branch router interfaces to help ensure the performance of latency-sensitive applications. The in- built redundancy and failover with fast convergence with the fast source to destination convergence ensures high availability and resilience. Finally, IPSec-VPN ensures tunneling without going through the gateway protocol [2,13].

3.6 SSL-VPN

IPSec –VPN provide security in the WMN from many attacks. IPSec sits at layer three of the stack and protects IP packets exchanged between remote networks or hosts and an IPSec gateway located at the edge of an organization's private network. But the SSL provides security at upper layer i.e transport layer ,session layer and application [20]. Both the IPSec-VPN and SSL-VPN provide authentication via certificate ,remote access ,defend from attacks and security while remote computer access . But SSL-VPN is better solution for as it provides non –certified user authentication . As WMN is a vast network which having much more users so SSL provides cheap mean of Security for WMN. Another thing is that IPSec VPNs are a common response to the remote access need, but for enterprises with a large contingency of mobile employees and/or business partners, they serve as little more than a band-aid. Excluding fixed, site-to-site connectivity, for which an IPSec VPN is an excellent solution, IPSec VPNs deployed to mobile users expose the network to security vulnerabilities. Additionally, they pose significant client and network problems for IT administrators when deployed to a large number of employees and/or corporate partners. As such, they impose significant limitations on the potential user base. IPSec with VPN need complex software installation. It may be possible to virus infection while with IPSec security. So there is also needed firewall protection with IPSec. But SSL is better solution for mobile users unlike IPSec VPN. Because SSL VPNs offer application-layer access and utilize SSL, there is no client software installation or server configuration changes required. As such, an SSL-based appliance can deploy secure remote access to thousands of users in about an hour as WMN support multiple users. Needless to say, this is significantly more cost-effective and time efficient than installing IPSec VPNs on dedicated machines, one by one. And because SSL VPNs leverage the strong security available in standard Web browsers, enterprises can have secure access without requiring dedicated laptops, additional security devices, or new software applications. Since SSL is a standard, ubiquitous protocol, users have no firewall traversal issues connecting with their networks from outside the LAN, and issues with service providers are void because users are going to a pre-defined URL so SSL VPN users cannot be blocked or charged additional fees when accessing their corporate networks from remote locations, as is the case with IPSec. SSL VPNs deliver secure remote access at reduced deployment cost and without the ongoing support and administration expenses associated with IPSec VPNs. So fulfill the need of WMN [21].

SSL VPN provided following security Services

- **Authentication**. Authentication is the process a VPN uses to limit access to protected services by forcing users to identify themselves. This feature includes the ability to support strong authentication and to integrate with current authentication mechanisms.

- **Encryption and integrity protection.** Encryption protects the confidentiality of data as it traverses the Internet, while integrity protection ensures that the data is not altered as it traverses the Internet. Both are inherent in SSL.

- **Access control**. Access control permits or restricts access to applications at a granular level, such as per-user, per-group, and per-resource.

- **Endpoint security controls**. Endpoint security controls validate the security compliance of the client system that is attempting to use the SSL VPN. For example, host integrity checks may verify that firewall, malware detection and antivirus software are enabled and running on the client system, and the host is up-to-date on its patches. Endpoint security controls also include security protection mechanisms, such as Web browser cache cleaners, that remove sensitive information from client systems.

- **Intrusion prevention**. Intrusion prevention involves inspecting the data after it has been decrypted in the SSL VPN for potential attacks. It may also include anti-malware functionality to detect viruses, worms, and other malicious payloads and block or change network access rights based on the results of such checks [22].

  So SSL VPN is a better solution over WMN to provide security.

4. Conclusion

WMN is a vast, heterogeneous, self configured and multi-hop network. Due to multi-hop and vast network, it is more vulnerable to many active as well as passive attacks. So there are many security mechanisms are implemented to secure the network and provide secure communication. The security is provided my many mechanisms via traffic engineering. Security is provided via MPLS-TE by fast data switching and repid autoconfigration of packet route. From passive attacks and security is also provided by secure tunnels with authentication, encryption by IPSec security and by SSL.

5. Acknowledgement

The authors are grateful to Saheed Bhagat Singh College of Engg. & Tech. ,Punjab(India) for providing continuous support throughout the work.

Reference

[1]. Ian F. Akyildiz, Xudong Wang , Weilin Wang “Wireless mesh Networks: A survey” Computer Network 2005; 47(4): 445-487.

[2]. Okechukwu E.muogilim, kok-keong loo , Richard comely “Wireless Mesh Network security: a traffic engineering management approach ” Journal of Network and Computer Applications 34 (2011) 478–491.

[3]. D. Cherubini , A.Fanni , A.Mereu , A.Frangioni , C.Murgia , M.G.Scutell, P.Zuddas “Linear programming models for traffic engineering in 100% survivable networks under combined IS–IS/OSPF and MPLS-TE” Computers & Operations Research 38 (2011) 1805–1815.

[4]. Amit Gaur, Abhinav Prakash, Saugat Joshi, Dharma P. Agrawal “Polynomial based scheme (PBS) for establishing Authentic Associations in Wireless Mesh Networks”

[5]. Jongtack Kim, Saewoong Bahk “Design of certification authority using secret redistribution and multicast routing in wireless mesh networks” Computer Networks 53 (2009) 98–109.

[6]. Levente Buttyán , László Dóra , Fabio Martinelli , Marinella Petrocchi “Fast certificate-based authentication scheme in multi-operator maintained wireless mesh network” Computer Communications 33 (2010) 907–922.

[7]. Serge-Paul Carrasco; Partner, Carrasco & Associates “MPLS VPN Services PW, VPLS and BGP MPLS/IP VPNs”: Technology White Paper, Copyright © 2003-2006.

[8]. Francesco Palmieri “VPN scalability over high performance backbones Evaluating MPLS VPN against traditional approaches” Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC’03) 1530-1346/03 $17.00 © 2003 IEEE.

[9]. Robert Cotter, Deep Medhi “Survivable Design of Reconfigurable MPLS VPN Networks” 978-1-4244-5048-0/09/ 26.00 c_2009 IEEE.

[10]. Mohamed EL Hachimi, Marc-Andr´e Breton, Maria Bennani ” Efficient QoS implementation for MPLS VPN” 978-0-7695-3096-3/08 $25.00 © 2008 IEEE DOI 10.1109/WAINA.2008.274.

[11]. .Nik Clayton, Free BSD Handbook available at:”www.freebsd,org/doc/en.us.ISO8859-1/book/handbook/ipsec,html.

[12]. Virtual private network consortium available at:” www.vpnc,org/vpn_standards.html”.

[13]. Guide to IPSec VPNs: Recommendations of the National Institute of Standards and Technology available at:” csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf” NIST Special Publication 800-77.

[14]. VPN Consortium Scenario 1: Gateway-to-Gateway with Preshared Secrets available at:”www.vpnc.org/InteropProfiles/FVS336G-profile.pdf”.

[15]. IPSec available at:”en. Wikipedia.org/wiki/ipsec”.

[16]. Kent, S.:Atkinson, R. (November 1998).” IP Authentication Header IETF ”.RFC2402.

[17]. Kent, S. (December 2005). “IP Authentication Header. IETF.” RFC 4302.

[18]. "Protocol Numbers". IANA. IANA. 2010-05-27. Archived from the original on 2010-07-27.

[19]. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei “chapter no-12 : A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks” available at: “citeseerx.ist.psu.edu/viewdoc”

[20]. *Ray Stanton, “securing VPNs : Comparing SSL and IPSec”* Computer Fraud & Security, Volume 2005, Issue 9, September 2005, Pages 17–19.

[21]. Andrew Harding, technical director,Neoteris, “*SSL Virtual Private Networks*” 0167-4048/03 ©2003 Elsevier Ltd.

[22]. B. Wu, J. Wu, E. Fernandez, S. Magliveras, Secure and efficient key management in mobile ad hoc wireless networks, in: Proceedings of the 19th IEEE International Parallel and Distributed Symposium (IPDPS 2005). The First International Workshop on Security in Systems and Networks (SSN 2005), 2005, p. 288.

[23]. S. Yi, R. Kravets, MOCA: mobile certificate authority for wireless ad hoc networks, in: Proceedings of the 2nd Annual PKI Research Workshop (PKI’03), 2003.

[24]. A. Shamir, How to share a secret, Communications of the ACM 22 (11) (1979) 612–613.

[25]. G.R. Blakley, Safeguarding cryptographic keys, in: Proceedings of the National Computer Conference, 1979.

[26]. Palmieri F. VPN scalability over high performance backbones evaluating MPLS VPN against traditional approaches. In: Proceedings of the eighth IEEE international symposium on computers and communications (ISCC), vol. 2, June–July 2003. p. 975–81.

[27]. IEEE Std 802.11iTM, Medium Access Control (MAC) security enhancements, amendment 6 to IEEE Standard for local and metropolitan area networks part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications (July 2004).

[28]. D.SPA.28, ECRYPT Yearly Report on Algorithms and Keysizes (2007–2008), IST- 2002-507932, ECRYPT, European Network of Excellence in Cryptology, 2008.

[29]. E. Rosen and R. Y. ”bgp/mpls vpns”. March 1999. Rfc RFC2547.

[30]. I. Askoxylakis, B. Bencsáth, L. Buttyán, L. Dóra, V. Siris, D. Szili, I. Vajda, Securing Multi-operator Based QoS-aware Mesh Networks: Requirements and Design Options, Wireless Communications and Mobile Computing (Special Issue on QoS and Security in Wireless Networks), 36 pp.

[31]. IEEE 802.11rTM-2008, IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 2: Fast BSS Transition (July 2008).

[32]. Naraghi-Pour M, Desai V. Loop-free traffic engineering with path protection in MPLS VPNs. Computer Networks 2008;22(12):2360–372.