Advances in Computer Science and its Applications (ACSA)
Vol. 1, No. 4, 2012, ISSN 2166-2924

www.worldsciencepublisher.org

Optimization of Security Mechanism to Enhance Data Access Speed in Wireless Mesh Networks

M.Sudha[1] M.Monica[2]

[1] Assistant Professor Senior, School of Information Technology & Engineering,
[2] Assistant Professor, School of Computing Sciences &Engineering,
VIT University, India

Email: msudha@vit.ac.in , monica.m@vit.ac.in

Abstract- Wireless mesh networks (WMN) are rapidly emerging as a promising complement to existing broad band access infrastructures; despite recent advances in wireless mesh networking, many research challenges still remain up in the air. WMNs are multi-hop networks consisting of two types of nodes, Mesh Routers and Mesh Clients. Mesh Routers are more static and less resource constrained than mobile Mesh Clients, both mesh router and mesh clients participate in the routing and forwarding of packets and forms the wireless backhaul of the network, hence Secure Routing in Hybrid Wireless Mesh networks is a challenging task. It is inevitable for any security framework to adapt an efficient low power high throughput encryption/decryption technique for resource constrained wireless mess nodes. In our proposed work novel sub pipelined architecture is adopted to optimize the existing Advanced Encryption Standard (AES) algorithm. The design can operate in non feedback mode and process blocks of data simultaneously. The proposed architecture is simulated in VHDL and implemented using Xilinx and our work addresses the overview of WMNs, the existing architecture followed by our proposed architecture for secure network access.

Keywords*:* WMN's (Wireless Mesh Networks); Mesh nodes; Advanced Encryption Standard (AES)

1. Introduction

As various wireless technologies evolve into the next generation to provide better services, a key technology, wireless mesh networks (WMNs), has emerged recently attracting significant interest from academia, industry, and standard organizations. WMNs are likely to resolve the limitations and to significantly improve the performance of existing ad hoc networks. WMNs will deliver wireless services for a large variety of applications in personal, local, campus, and metropolitan areas. In WMNs, nodes are comprised of mesh routers and mesh client, where mesh routers have minimal mobility and form the backbone of WMNs. Each node operates not only as a host but also as a router, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations. The integration of WMNs with other networks such as the Internet, cellular, IEEE 802.11, IEEE 802.15, IEEE 802.16, etc. can be accomplished through mesh routers. Mesh clients can be either stationary or mobile, and can form a client mesh network among themselves and with mesh routers. A WMN is dynamically self-organized and self configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves. This feature brings many advantages to WMNs such as low up-front cost, easy network maintenance, robustness, and reliable service coverage. Conventional nodes (e.g., desktops, laptops, PDAs, PocketPCs, phones, etc.) equipped with wireless network interface cards (NICs) can connect directly to wireless mesh routers. Customers without wireless NICs can access WMNs by connecting to wireless mesh routers through, for example, Ethernet. Thus, WMNs will greatly help the users to be always-online anywhere anytime. Moreover, the gateway/bridge functionalities in mesh routers enable the integration of WMNs with various existing wireless networks such as cellular, wireless sensor, wireless-fidelity (Wi-Fi) and worldwide inter-operability for microwave access (WiMAX), and WiMedia networks.

WMN is a promising wireless technology for numerous applications [1], e.g., broadband home networking, community and neighborhood networks, enterprise networking, building automation, etc. It is gaining significant attention as a possible way for cash strapped Internet service providers (ISPs), carriers, and others to roll out robust and reliable wireless broadband service access in a way that needs minimal up-front investments. With the capability of self organization and self configuration, WMNs can be deployed incrementally, one node at a time,

as needed. As more nodes are installed, the reliability and connectivity for the users increase accordingly. [3] Deploying a WMN is not too difficult, because all the required components are already available in the form of ad hoc network routing protocols. Based on the literature survey we found that considerable research efforts are still needed. For example, the available routing protocols applied to WMNs do not have enough scalability; the throughput drops significantly as the number of nodes or hops in a WMN increases, Security need to be enhanced or re-invented. Researchers have started to revisit the security models and the various protocol designs of existing wireless networks, especially of IEEE 802.11 networks and ad hoc networks; from the perspective of WMNs.The section 2 describes the characteristic of WMNs followed by the existing and proposed architecture in section 3 and 4, Section 5 and 6 presents our security policy and requirements proposed to ensure speed and security in wireless mesh.

2. Wireless Mess Networks Characteristics

One of the key features of WMNs is the ability to dynamically self-organize and self-configure. The nodes in a WMN automatically detect neighbor nodes and establish and maintain network connectivity in an ad hoc fashion. This is typically implemented at the network layer through the use of routing protocols. WMNs self-configuring nature allows easy and rapid deployment in an emergency. WMNs can also dynamically adapt to changing environments and essentially self-heal in case of node or link failures. This self-healing capability combined with the mesh topology's inherent redundancy provides wireless mesh networks with a high level of robustness and fault tolerance.

Wireless networks are easy to install, In contrast with installing a wired network, which needs significant knowledge, hardware, money and time, a wireless network access point is cheap, and can be installed very easily without much technical knowledge[2]. The access point is just plugged into the wired network. This means that rogue (unauthorized) access points can be installed very easily, without proper authorization and configuration, and in that way become a potential unauthorized point into the wired network. Because of this ease of implementation of wireless networks, very often no proper risk analysis is done before any wireless facilities are installed, and such networks can create large risks to the corporate network. Furthermore, very often the wireless access point is connected to the wired network behind the company firewall, which increases the risks significantly.

3. Existing System Model

WMNs architecture is of three types based on functionality of mesh nodes as Infrastructure Mesh, Client Mesh and Hybrid Mesh.

3.1 Infrastructure Mesh Architecture

Infrastructure WMNs includes mesh routers forming an infrastructure for clients that connect to them. The infrastructure Meshing can be built using various types of technologies as the Internet, cellular, IEEE 802.11, IEEE 802.15 etc, the mesh routers form a mesh of self-configuring, self-healing links among themselves as in the Figure-1. Using the gateway functionality, mesh routers can be connected to the Internet this approach, also referred to as infrastructure meshing, provides backbone for conventional clients and enables integration of WMNs with existing wireless networks, through gateway or bridge functionalities in mesh routers.

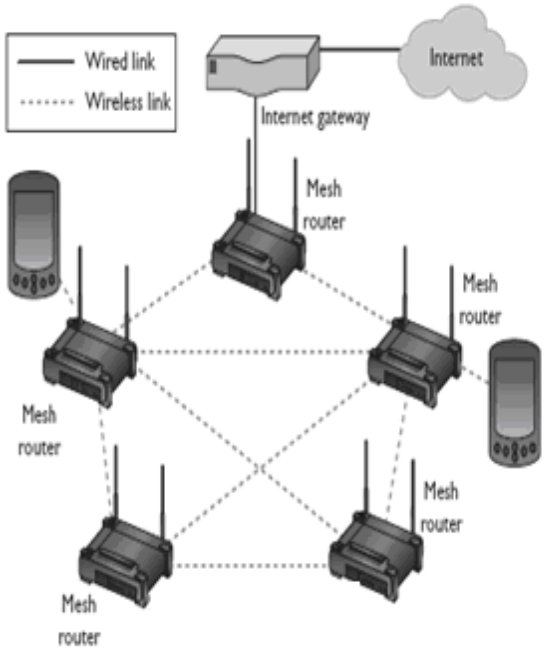


Figure-1 Infrastructure-Meshing

Conventional clients with Ethernet interface can be connected to mesh routers via Ethernet links. For conventional clients with the same radio technologies as mesh routers, they can directly communicate with mesh routers. If different radio technologies are used, clients must communicate with the base stations that have Ethernet connections to mesh routers. Infrastructure WMNs are the most commonly used type. For example, community and neighborhood networks can be built using infrastructure meshing.

3.2 Client Mesh Architecture

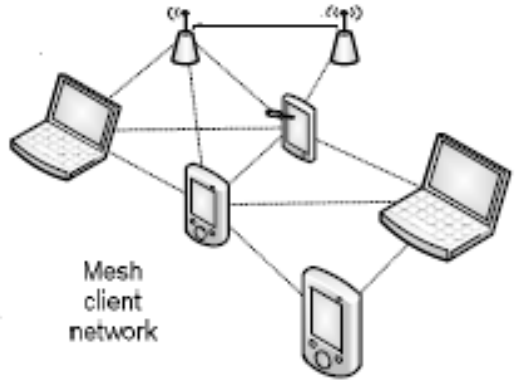


Figure-2 Client-Meshing

Client Mesh architecture provides peer-to-peer networks among client devices it is similar to the existing ad-hoc networks. In this type of architecture, client nodes constitute the actual network to perform routing and configuration functionalities as well as providing end-user applications to customers. Hence, a mesh router is not required for these types of networks. A packet destined to a node in the network hops through multiple nodes to reach the destination. Client WMNs are usually formed using one type of radios on devices. Moreover, the requirements on end user devices is increased when compared to infrastructure meshing, since, in Client WMNs, the end-users must perform additional functions such as routing and self-configuration.

3.3 Hybrid Mesh Architecture

Hybrid Mesh architecture is the combination of infrastructure and client meshing, Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. While the infrastructure provides connectivity to other networks such as the Internet, Wi-Fi, WiMAX, cellular, and sensor networks; the routing capabilities of clients provide improved connectivity and coverage inside the WMN. The hybrid architecture will be the most applicable case in our opinion.

4. Proposed System Model

The proposed SHA- Secure Hybrid architecture is more over similar to the existing architecture with some optimization, In this SHA a Master Mesh Router and a Master Mesh client is proposed in addition to the Mesh routers and Clients, Master Mesh Router (MMR) is the router that remains stable in the network it contains list of the entire mesh router in that network and maintains a clear client table for efficient network access, based on the proposed security policy the secure network access can be ensured using this Master Mesh Router, the proposed Master Mesh client which can reduce the overhead at individual mesh nodes.

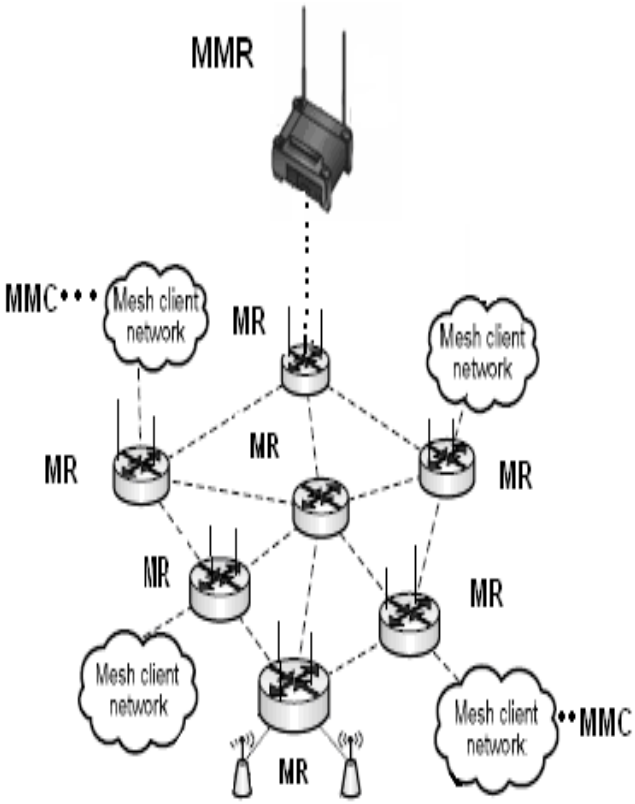


Figure-4 Proposed Hybrid-Meshing

Master mesh Client contain the list of registered clients that can access the network for data transfer, resource sharing after getting network access authentication from Master Mesh Router, a Master Mesh client (MMC) is a the node that remains stable in the WMNs for some period of time which can be used to maintain the cache table that defines the most recently visited paths using peer neighbor nodes. AES is used for our architecture to ensure both authentication and confidentiality based on the framed security policies.

5. Proposed Framework Implementation

WMNs have become popular because of this low cost and convenience, It is so much easier to plug in a WAP than to run 100 feet of cable, but still have no appreciation for the security measures, also this wireless mesh is more vulnerable to critical network access threats, why we chose AES (Advanced Encryption standard) algorithm, Initially keeping the security as the important need WEP was widely used but recently researchers at UC Berkley (www.cs.berkeley.edu /isaac/ wepfaq. htm) have shown WEP security can be broken by cryptanalysis or by an efficient hacker. For the above mentioned limitation, we have proposed to use a security risk resilient algorithm for

the proposed hybrid meshing; AES is block cipher that processes plain text in 128 bit blocks, using following 128 bit, 256 bit keys. We focus on investigating network access security in this work using AES with 128 bit keys; and have planned to leave the exploration of the other issues as future work with respect to network access security.

5.1 Access security policy

Step 1: Effective procedures for secure access.
Step 2: Significance of the data transmitted across the networks.
Step 3: Optimized Encryption techniques to enforce safety.
Step 4: Check the circumstances of adding a new client on the network.

5.2 Functional Process

The designated Master Mesh Router (MMR) must perform the following security requirements as series of steps to ensure secure access. Network Accessing can be performed as follows, First, a Symmetric Master Key is generated and shared with MRs initially at the time of setup, symmetric key Possessed by the MMR and Mesh Router is used for the positive access decision which is done by passing initial Hello message for further mesh nodes communication, to avoid unauthorized imposition of routers or access points accessions in to the network. Secondly, a temporal symmetric key issued to the MR and to the individual MC is used for data confidentiality, these keys are renewed after specific or random intervals of time based on the mesh nodes interaction, and initially for simplicity we have assumed mesh clients to be less mobile.

Network access security is much more difficult to ensure in WMNs, [6] one major reason is that mesh routers are designed to accept open access requests by most likely unknown mesh clients this causes security backhaul that can be solved using the proposed SHA, the dynamic network topology caused by the mobility of mesh clients can make the key issue process quite challenging which is proposed as follow up of our research work. The available University test Beds for WMNs simulations are, Georgia Tech - BWN-Mesh, MIT – Roofnet, Rutgers –Win Lab, Orbit SUNY Stony brook and Hyacinth University of Utah – Emulab.so far we have designed a simplified AES architecture that can be used for this wireless nodes association and the SHA implementation is in progress the simulation results are yet to be analyzed.

6. Architectural Optimization of AES

AES also referred as Rijndael algorithm is a block cipher algorithm that has been developed by Joan Daemon and Vincent Rijmen [1]. The Rijndael algorithm is an iterated block cipher with variable key length and variable block length. The block and the key length can be independently specified to 128,192 or 256 bits.

The algorithm consists of:
1. An initial data/key addition
2. Nine (128-bits), eleven (192-bits) or thirteen (256-bits) rounds of standard round
3. A final round, which is a variation of a standard round.
4. The number of standard rounds depends on the block and key length.

The initial key is expanded to generate the round keys, each of size equal to 128 bits. Each round of the algorithm receives a new round key from the key schedule module; the number of standard rounds depends on the block and key length. The initial key is expanded to generate the round keys, each of size equal to block length. In this 128-bit block Rijndael algorithm, plain text and cipher text are processed in blocks of 128 bits. A data block to be encrypted is split into an array of bytes, and each encryption operation is byte-oriented. The algorithm has different transformations to be applied on the data block and the intermediate result is called State. Both the Key State and the Block State are arranged in column major order.

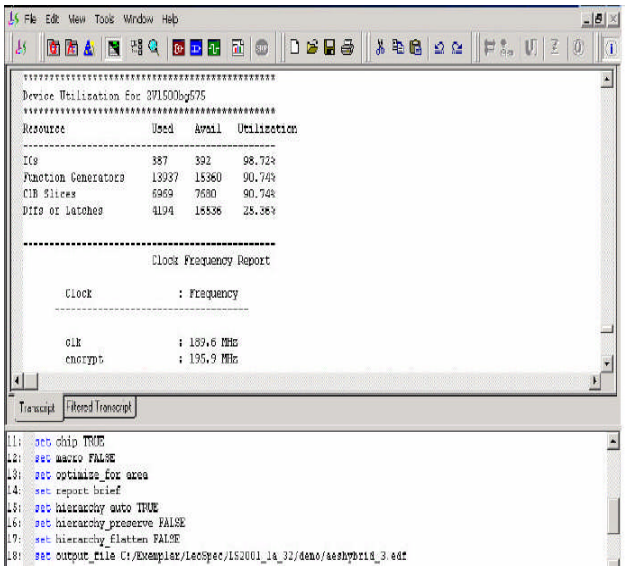
The intermediate round values are represented as a Block State matrix of (4*4) bytes, the initial and round keys of size 128 bits are represented as a Key State matrix of (4*4) bytes, Hence for 128 bit block and 128 bit key. The central design principle of the AES algorithm is simplicity this facilitates implementations on different platforms under different sets of constraints. [8] The simplicity is achieved by two means: the adoption of symmetry at different levels and the choice of basic operations. The first level of symmetry lies in the fact that the AES algorithm encrypts 128-bit blocks of plaintext by repeatedly applying the same round transformation, outlined in figure 2, AES-128 applies the round transformation 10 times.

The proposed optimization is implemented using sub-pipelined architectural mode, similar to pipelining, sub pipelining also inserts rows of registers among combinational logic but in this case, registers are inserted both between and inside each round unit. If each round unit can be divided in to r stages with equal delay, it is that a k round of a sub pipelined architecture can approximately achieve r times the speed of k round. The speed up of a k-round sub pipelined architecture with r=2 is given by throughput sub pipe/throughput basic, throughput = (block size)/ total clock, where total clock is the delay of the single round

Therefore the adoption of this optimized architecture of AES for the proposed SHA for performing Mesh router authorization can ensure data confidentiality among the communicating mesh nodes in the hybrid architecture with enhanced speed. This optimized AES design is verified using ModelSim and Leonardo spectrum, the synthesis and

comparison chart are given below for the reference. Existing clock frequency is in the range above our proposed model which yields fewer throughputs than our proposed architectural model.

6.1 Simulation and Synthesis Report



Clk: 150 MHz (Frequency)

7. Conclusion

Wireless networks can be a significant tool in increasing business productivity. However, as discussed above, wireless networks bring with it a totally new set of security risks which must be evaluated and countered although with current technology there is no reason not to trust a well setup wireless network. Insecure wireless networks can cause very serious risks to companies and before installing any such networks, all these risks must be identified, evaluated, and based on the results, the necessary counter measures must be installed to secure the network. In this paper, we have presented the proposed architecture that can avoid rogue access points threats in wireless mesh networks. Proposed SHA scheme is hybrid in nature finding the secure way to deliver the data in different format such as images to the destination. Also the proposed security mechanism can sufficiently decrease the overhead induced at mesh routers. Thus our enhanced model for WMNs ensures data confidentiality as well fast access by efficiently utilizing the characteristics of sub pipelining.

References

[1] M.Sudha, M.Monica: “Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography”, Advance in Computer Science Application, Vol. 01, No. 01, pp 32-37, March 2012.

[2] Ian F. Akyildiz, Xudong Wang, Weilin Wang,"Wireless mesh networks: a survey", Computer network 47, 2005

[3] Securing Wireless Mesh Networks *in IEEE Wireless Communications*, vol. 13, no. 2, pp. 50 – 55, April 2006, by Naouel Ben Salem Jean-Pierre Hubaux, EPFL Lausanne, Switzerland

[4] Y.-Ch. Hu and A. Perrig. “A Survey of Secure Wireless Ad Hoc Routing”. IEEE Security and Privacy, special issue on Making Wireless Work, vol. 2, no. 3, 2004.

[5] J. Hauser, “IEEE 802.11 ESS Mesh,” draft IEEE 802.11-03/ 759r2, IEEE, 2003.

[6] K. Ramachandran et al., “On the Design and Implementation of Infrastructure Mesh Networks,” *Proc. IEEE Workshop on Wireless Mesh Networks* (WiMesh), IEEE CS Press, 2005, pp. 4–15.

[7] Secure Routing in Wireless Mesh Networks by S. Asherson, A. Hutchison. {Sasherso, hutch} @cs.uct.ac.za Department of Computer Science University of Cape Town.

[8] AES web site of ECRYPT: www.iaik.tugraz.ac.at/ research/ krypto/ AES.

[9] Yudong Zhang, Lenan Wu, Face Pose Estimation by Chaotic Artificial Bee Colony, International Journal of Digital Content Technology and its Applications, 5(2) (2011) 55-63.

[10] Yudong Zhang, Lenan Wu, A Rotation Invariant Image Descriptor based on Radon Transform, International Journal of Digital Content Technology and its Applications, 5(4) (2011) 209-217.

[11] Yudong Zhang, Lenan Wu, Geng Wei, A New Classifier for Polarimetric SAR Images, Progress in lectromagnetics Research, 94 (2009) 83-104.