ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Elliptic Curve Riddle Hiding Scheme for Preventing Selective Routes in Wireless Mesh Networks

M.D.Vasanthi[1], B.Prakash[2]
Department of CSE, Adhiparasakthi Engineering College, Melmaruvathur, Tamilnadu, India[1, 2]

Abstract— Mesh Networking is based on routing techniques originally developed for battlefield communications. By pushing intelligence decision making to the edge of network, high performance and scalable networks can be built at very low cost. Mesh networking play an important role in the wireless community. It promises self-healing, multi-hop networking capability that lowers node costs and power consumption, and increase reliability in a real-world noisy environment. The problem of selective routing path in wireless mesh networks, in these paths, the adversary is active only for a short period of time, selectively targeting messages of high importance. Thereby the advantages of selective routes in terms of network performance degradation and adversary effort by presenting two case studies; a selective path on TCP and one on routing. The selective routing can be launched by performing real-time packet classification at the physical layer. To mitigate from the attacks, there are three schemes that prevent real-time packet classification by combining ECC cryptographic primitives with physical layer attributes. Thus here the security and evaluation of computational and communication overhead is analyzed.

Keywords —WMN, Channel Allocation System, Hiding Scheme, Encryption techniques.

I. INTRODUCTION

Infrastructure Wireless Mesh Networks (WMNs) have been increasingly deployed and widely used for various purposes such as broadband Internet access or mobile telephony backhauling. Compared to traditional single hop WiFi networks, the WMN deployments are more flexible and self-configured. Wireless coverage can be easily extended by adding more wireless mesh routers to form a wireless infrastructure. With multiple radios, a capacity gain cannot be fully realized, however, if the issues related to routing, link scheduling and channel assignment (CA) (i.e., mapping of channels to radios at each node) are not properly addressed. In fact, routing and CA are mutually dependent and normally considered jointly. While CA determines the capacity of each link in a network, routing determines the traffic rate at each link. CA decisions thus affect routing decisions inevitably.

As various wireless networks evolve into the next generation to provide better services, a key technology, wireless meshes networks which use mesh networking, has emerged recently. In mesh networking, nodes are comprised of mesh routers and mesh clients. 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. A mesh network is dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves (creating, in effect, an ad hoc network). So mesh networking has to manage a network, which is highly dynamic, in terms of topology, location of nodes and routing path.

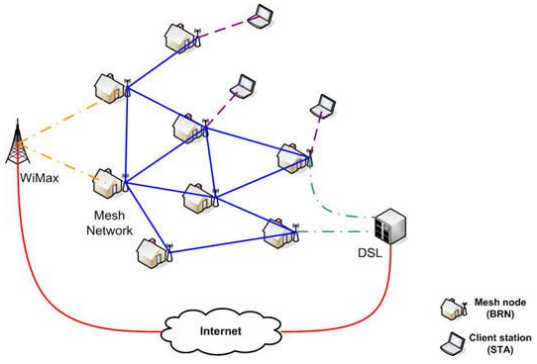

Figure 1. Wireless Mesh Network.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

A. Unique Features of WMN

- *Reliability:*
  Inherently shortens the distance between application end-points (in terms of improving link quality)by increasing the link to-link receive 'signal to noise ratio.
- *Redundancy:*
  Provides alternate path ways throughout the mesh network in the event a router fails (local noise burst, loss of power, hardware failure, etc.)
- *Penetration:*
  Prevents the negative effects of temporary fading, radio shadows, and noisy environments, which are inherent in wireless systems.
- *Coverage:*
  Attaining greater communications reach with the support of intermediate routers.

II. RELATED WORK

In path based approach, in which packet or data flow in a same way while transmitting the file. During transmission of data any router fails or hijacked by any attacker then the data will not reach the destination in a successful way.

The router will continuously transmits any file to the receiver to make the traffic overhead and corrupts the system. It will be easy for attacker to hack the file and sends the modified data to the receiver.

An adaptive dynamic channel allocation protocol to be used on dynamic interfaces. Compared with MMAC, ADCA reduces the packet delivery delay without degrading the network throughput. In addition an interference and congestion aware routing algorithm in the hybrid network, which balances the channel usage in the network and therefore increases the network throughput.

The packet can flow in a dynamic path so that attacker will not have knowledge about path in which the packet has been transferred. Then to make it efficient, password protection has been given to the packet.

The route data that has been received by the receiver will be filtered and if there has been any malicious file it will detect that file before receiving by the receiver.

The Selective routes in which specific messages of "high importance" are targeted. This must be capable of implementing a "classify-then-route" strategy before the completion of a wireless transmission. Classifying transmitted packets using protocol semantics, or by decoding packets on the fly using ECC. Selective route requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.

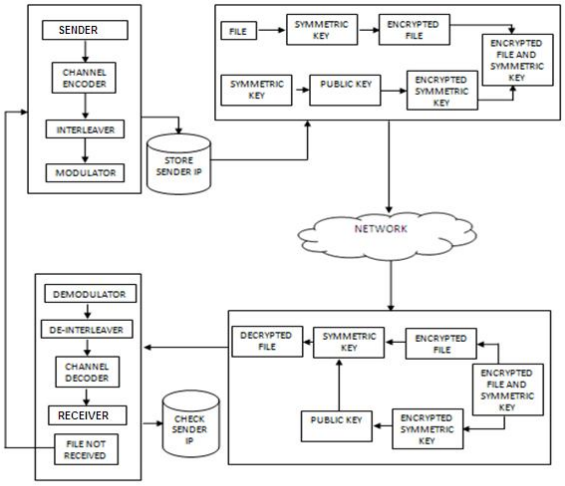

Figure 2. Architecture For Packet Encryption

The packet will be encrypted using DES/ Rijndael algorithm, then this key will be encrypted using RSA algorithm (dual encryption has been done) for an efficient transmission of packet.

Algorithm 1

ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curves are used to construct the public key cryptography system. The private key d is randomly selected from [1,n-1], where n is integer. Then the public key Q is computed by dP, where P,Q are points on the elliptic curve. Like the conventional cryptosystems, once the key pair (d, Q) is generated, a variety of cryptosystems such as signature, encryption/decryption, key management system can be set up. Computing dP is denoted as scalar multiplication. It is not only used for the computation of the public key but also for the signature, encryption, and key agreement in the ECC system.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Key Generation:

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.
Now, we have to select a number 'd' within the range of 'n'.
Using the following equation we can generate the public key Q = d * P
d = The random number that we have selected within the range of (1 to n-1). P is the point on the curve.
'Q' is the public key and 'd' is the private key.

Encryption:

Let 'm' be the message that we are sending. We have to represent this message on the curve. These have in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Consider '*m*' has the point '*M*' on the curve '*E*'. Randomly select 'k' from [1 - (n-1)].
Two cipher texts will be generated let it be C1 and C2.
C1 = k*P
C2 = M + k*Q
C1 and C2 will be send

Decryption:

Have to get back the message 'm' that was send to us,
M = C2 – d * C1
M is the original message that we have send.

1) Proof

How does we get back the message,
M = C2 – d * C1
'M' can be represented as 'C2 – d * C1′
C2 – d * C1 = (M + k * Q) – d * (k * P) (C2 = M + k * Q and C1 = k * P)= M + k * d * P – d * k *P (canceling out k * d * P)= M (Original Message)

III. PACKET HIDING TECHNIQUES

The packets are pre-processed by a hiding the packets of the before transmission but remain unencrypted. The route cannot perform packet classification until all pseudo-messages corresponding to the original packet have been received and the inverse transformation has been applied. It's working on the condition but the data to be hiding on to the network.

IV. RIDDLE GENERATING SCHEME

A sender S has a packet m for transmission. The sender selects a random key k, of a desired length. S generates a riddle (key, time), where riddle () denotes the riddle generator function, and tcp denotes the time required for the solution of the riddle. In this riddle generator used for avoiding the route flooding on the network. It's to be resolving the riddle generating of attacking time of the scheme.

V. CONCLUSION

The impact of selective path on network protocols such as TCP and routing. The packet can flow in a dynamic path so that attacker will not have knowledge about path in which the packet has been transferred. Then to make it efficient, password protection has been given to the packet. This shows that a selective path can significantly impact performance with very low effort. There are three schemes that transform a selective path to a random one by preventing real-time packet classification.

REFERENCES

[1] M. Alicherry, R. Bhatia, and L. Li, "Joint Channel Assignment and Routing for Throughput Optimization in Multi-Radio Wireless Mesh Networks,"Proc. ACM MobiCom,2005.
[2] Y. Ding, K. Pongaliur, and L. Xiao, "Hybrid Multi-Channel MultiRadio Wireless Mesh Networks," Proc. IEEE 17th Int'l Workshop Quality of Service (IWQoS), 2009.
[3] R. Draves, J. Padhye, and B. Zill, "Comparison of Routing Metrics for Static Multi-Hop Wireless Networks," Proc. SIGCOMM, 2004.
[4] R. Draves, J. Padhye, and B. Zill, "Routing in Multi-Radio MultiHop Wirelss Mesh Networks," Proc. ACM MobiCom, 2004.
[5] P. Dutta, S. Jaiswal, and R. Rastogi, "Routing and Channel Asslocation in Rural Wireless Mesh Networks," Proc. IEEE INFOCOM, 2007.
[6] "Hyacinth: An IEEE 802.11-Based Multi-Channel Wireless Mesh Network," http://www.ecsl.cs.sunysb.edu/multichannel, 2012
[7] A. Raniwala, K. Gopalan, and T. Chiueh, "Centralized Channel Assignment and Routing Algorithms for Multi-Channel Wireless Mesh Networks,"ACM Mobile Computing and Comm. Rev.,vol. 8, pp. 50-65, 2004.
[8] A. Raniwala and T. Chiueh, "Architecture and Algorithms for an IEEE 802.11-based Multi-Channel Wireless Mesh Network,"Proc. IEEE INFOCOM,2005.
[9] J. Tang, G. Xue, and W. Zhang, "Interference-Aware Topology Control and QoS Routing in Multi-Channel Wireless Mesh Networks,"Proc. ACM MobiHoc,2005
[10] S.-L. Wu, C.-Y. Lin, Y.-C. Tseng, and J.-P. Sheu, "A New MultiChannel Mac Protocol with On-Demand Channel Assignment for Multi-Hop Mobile Ad Hoc Networks,"Proc. Int'l Symp. Parallel Architectures, Algorithms, and Networks (ISPAN),2000.