iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3209

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

A Review on Secure VPN using Network IPV6 based Moving Target Defense

Geethamani G.S [1], Subhashree.S [2]
[1]*Assistant Professor, PG Department of (IT), Hindusthan College of Arts and Science, Coimbatore*
[2] *PG Student, Department of (IT) , Hindusthan College of Arts and Science, Coimbatore.*

Abstract: In this paper, we introduce MVPN, a framework for building secure Virtual Private Networks (VPNs) with a novel Mobile IPv6 based Moving Target Defense strategy. Our approach aids in combating remote attacks against a VPN server. By eliminating the static address of the server, we make it difficult for an attacker to find the server. The server's address is randomly changed at a certain interval creating a moving target. At the same time, authenticated clients are updated through the use of the Binding Update procedure (standard Mobile IPv6 protocol). One key strength of this approach lies in the fact that the clients do not need to make any changes or use special software. Introducing Moving Target IPv6 Defense (MT6D) that hides and rotates IPv6 tasks by implementing MT6D tunneled packets. To form the tunnels, MT6D requires the endpoint interface identifier, a secret key and a nonce which makes them difficult to deploy in existing networks. In effect, data is encrypted at sender's side and forwarded via "tunnel "which is then decrypted at receiver's side. A remote-access VPN allows individual uses to establish secure connection with a remote computer network. These users can access the secure resources on that network as if they were directly plucked in to the networks services.
Index Terms: VPN-IPSC, SSL, VPN, Protocol IPV6 Architecture.

I. INTRODUCTION

Virtual private Network (VPN) is promptly growing technology which plays a great role in Wireless LAN (WLAN) by providing secure data transmission. The purpose of VPN is to provide safe and secure communication by creating virtual tunnels among pair of hosts on one occasion tunnel is created data transfer can take place. This paper presents anall-inclusive study of VPN-IPSC and VPN, IPV6 architecture and protocols used.VPN is based on the idea of tunneling. VPN tunneling implicates beginning and maintaining a logical network connection (that may contain intermediate hops). On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other base or carrier protocol, then transmitted between VPN client and server, and finally de-encapsulated on the receiving side. For Internet-based VPNs, packets in one of several VPN protocols are encapsulated within Internet Protocol (IP) packets. VPN protocols also support authentication and encryption to keep the tunnels secure. Virtual Private Networks (VPNs) are commonly used as a means to establish secure connections across the public network. For the computers that are connected through secure tunnels, the VPNs provide private network-like confidentiality and authentication. Though location anonymity is not guaranteed, the security and privacy of the communication is increased. Furthermore, allowing authenticated remote access to resources considered internal to an organization is one of the key advantages of using VPNs. Though, a legal client may share the server's IP with an external attacker. So the server cannot find the malicious client and put it in the black list. To solve this problem, as the second contribution, multiple IPs is considered on the server and an IP per each client is assigned in this new version. Therefore, if IDS detects an attack to a specific IP of the server, we can find the client that is sharing the server's IP with the attacker and put it in the black list.

A. VPN

Virtual private networks (VPNs) are point-to-point connections across a private or public network, such as the Internet. A VPN client uses special TCP/IP-based protocols, called tunneling protocols, to make a virtual call to a virtual port on a VPN server. In a typical VPN deployment, a client initiates a virtual point-to-point connection to a remote access server over the Internet. The remote access server answers the call, authenticates the caller, and transfers data between the VPN client and the organization's private network.

There are two types of VPN connections:

1) Remote access VPN
2) Site-to-site VPN

1) *Remote access VPN:* Remote access VPN connections enable users working at home or on the road to access a server on a private network using the infrastructure provided by a public network, such as the Internet. From the user's perspective, the VPN is a point-to-point connection between the computer (the VPN client) and an organization's server. The exact infrastructure of the shared or public network is irrelevant because it appears logically as if the data is sent over a dedicated private link.
2) *Site-to-site VPN:* Site-to-site VPN connections (also known as router-to-router VPN connections) enable organizations to have routed connections between separate offices or with other organizations over a public network while helping to maintain secure communications. A routed VPN connection across the Internet logically operates as a dedicated wide area network (WAN) link. When networks are connected over the Internet, as shown in the following figure, a router forwards packets to another router across a VPN connection. To the routers, the VPN connection operates as a data-link layer link.

A site-to-site VPN connection connects two portions of a private network. The VPN server provides a routed connection to the network to which the VPN server is attached. The calling router (the VPN client) authenticates itself to the answering router (the VPN server), and, for mutual authentication, the answering router authenticates itself to the calling router. In a site-to site VPN connection, the packets sent from either router across the VPN connection typically do not originate at the routers.

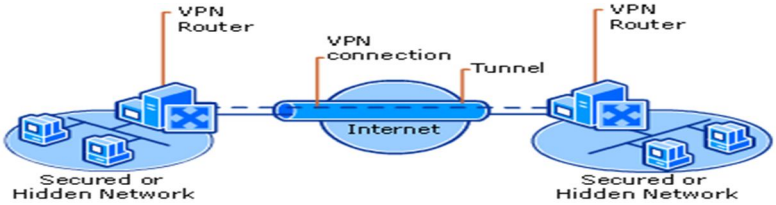


Figure 1: VPN Connecting Two Remote Sites across the Internet

II. DESIGN

The core of this approach involves the use of multiple IPv6 CoAs. The HoA is used as the enduring address of the server and the CoAs are used as the dynamic addresses. Each CoA is assigned to each client. A pseudo-random IP addresses are generated to dynamically rotate all CoAs of the server after each shuffling interval. During each of this shuffling interval, a new CoA is assigned to each client. The binding update mechanism is used to update clients with the new CoAs. According to the multiple CoA registration rules of MIPv6, the server (acting as if it were a mobile node) will send Binding Update (BU) messages to its clients to inform them of the new CoAs. When each client receives the BU, the HoA and CoA of the server are inserted into the binding cache. The server also removes the previous CoAs. Because of using IPsec for route optimizations, the home agent is not needed HoA is not accessible through the Internet, so a new client cannot start a connection to the server using the HoA of the server. Instead, the connection initiation is made by the server upon receiving an out- of-band request from a client (email can be used for this purpose). When a connection request is received from a new client, the server will ping the client and, according to the standard MIPv6 procedure, the server will start the route optimization mechanism and update the client with one of its active CoAs. The server has a table to save the list of clients and their mode includes normal mode, suspicious mode, and malicious mode. The default mode for a new client is normal mode. We have different shuffling interval for each mode. The shuffling interval for normal mode (tn) is longer than the shuffling interval for suspicious mode (ts). For isolating attackers, IDS should be installed on the server. If the IDS detect an attack, it reports the attacked IP to MVPN. When MVPN receives this attacked IP, it can find the responsible client because only one client knows this IP. However, it is too early to judge the client because the attacked IP might be detected by an attacker using IP scanner. So the server should put this client in suspicious mode and decrease the shuffling interval (using stinted of tn) for this client. If a new attack comes to the IP assigned to the suspicious client, then the server should put the client in malicious mode and remove the attacked IP and stop updating the malicious client with the new CoA. The IP of the malicious client can be removed from the blacklist manually by the security administrator. For updating the shared symmetric key, IPsec with Internet Key Exchange version 2 (IKEv2) should be used. So the keys will be updated and we can also prevent replay attacks.

A. VPN Tunneling

VPN supports two types of tunneling - voluntary and compulsory. Both types of tunneling are commonly used.

In voluntary tunneling, the VPN client manages connection setup. The client first makes a connection to the carrier network provider (an ISP in the case of Internet VPNs). Then, the VPN client application creates the tunnel to a VPN server over this live connection. In compulsory tunneling, the carrier network provider manages VPN connection setup. When the client first makes an

ordinary connection to the carrier, the carrier in turn immediately brokers a VPN connection between that client and a VPN server. From the client point of view, VPN

B. VPN Tunneling Protocols

Several computer network protocols have been implemented specifically for use with VPN tunnels. The three most popular VPN tunneling protocols listed below continue to compete with each other for acceptance in the industry. These protocols are generally incompatible with each other.

1) *Point-to-Point Tunneling Protocol (PPTP):* Several corporations worked together to create the PPTP specification. People generally associate PPTP with Microsoft because nearly all flavors of Windows include built-in client support for this protocol. The initial releases of PPTP for Windows by Microsoft contained security features that some experts claimed were too weak for serious use. Microsoft continues to improve its PPTP support, though.
2) *Layer Two Tunneling Protocol (L2TP):* The original competitor to PPTP for VPN tunneling was L2F, a protocol implemented primarily in Cisco products. In an attempt to improve on L2F, the best features of it and PPTP were combined to create a new standard called L2TP. Like PPTP, L2TP exists at the data link layer (Layer Two) in the OSI model -- thus the origin of its name.In this work we described three key properties for net-work moving target defense protocol solution or simply as the encryption scheme within L2TP or PPTP. IPsec exists at the network layer (Layer Three) of the OSI model.

While a lot of important information is being sent and received on the Internet, the information could be exposed to many threats, and the more the multicast service is various and generalized, the more the service range is widened. When a new member joins in or leaves from the multicast group, the group key, which the existing member used, should be newly updated. The existing method had a problem that the performance was depreciated by the key exchanging. This paper proposes the effective group management mechanism for a secure transmission of the multicast data on the multicast group.

III. IMPLEMENTATION

Four routers and eight computers running Ubuntu 14.04are used. An open source implementation of MIPv6 (UMIP) for Linux was used. Router R1 is used to emulate the heart of the Internet. The server's HoA does not have the same prefix with the advertised prefix of R2. So the server registered a CoA on R2 per each new client and updated the client with the new CoA. When the server changes its CoAs, it should update all clients with the new CoAs. During this procedure, all packets sent by clients will be dropped because are removed in the server's interface. For TCP test, a client generates and sends TCP packets to the server. During50 seconds, the client sends 1000 TCP packets per second to the server. During the handoff delay TCP experiences timeout, resends the unacknowledged packet(s) and goes to slow start.

A. VPN connections that use PPTP, L2TP/IPsec, and SSTP have the following properties:

1) Encapsulation
2) Authentication
3) Data encryption

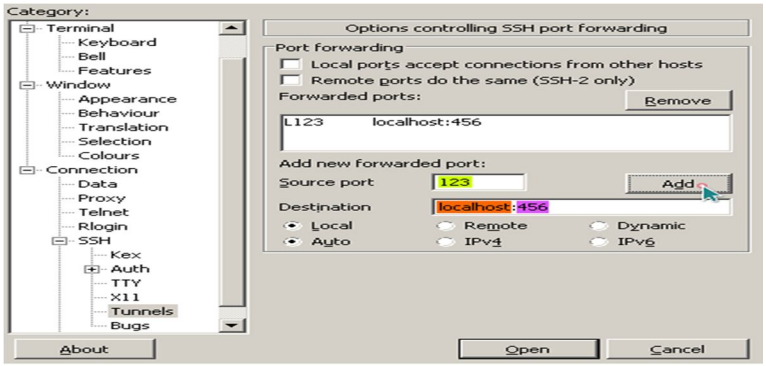


Figure: 2 Local ports forwarding with Ssh via command line.

B. Encapsulation

With VPN technology, private data is encapsulated with a header that contains routing information that allows the data to traverse the transit network. For examples of encapsulation, see VPN Tunneling Protocols.

C. Authentication

Authentication for VPN connections takes three different forms:

1) *User-level authentication by using PPP authentication:* To establish the VPN connection, the VPN server authenticates the VPN client that is attempting the connection by using a Point-to-Point Protocol (PPP) user-level authentication method and verifies that the VPN client has the appropriate authorization. If mutual authentication is used, the VPN client also authenticates the VPN server, which provides protection against computers that are masquerading as VPN servers.
2) *Computer-level authentication by using Internet Key Exchange (IKE):* To establish an Internet Protocol security (IPsec) security association, the VPN client and the VPN server use the IKE protocol to exchange either computer certificates or a preshared key. In either case, the VPN client and server authenticate each other at the computer level. Computer certificate authentication is highly recommended because it is a much stronger authentication method. Computer-level authentication is only performed for L2TP/IPsec connections.

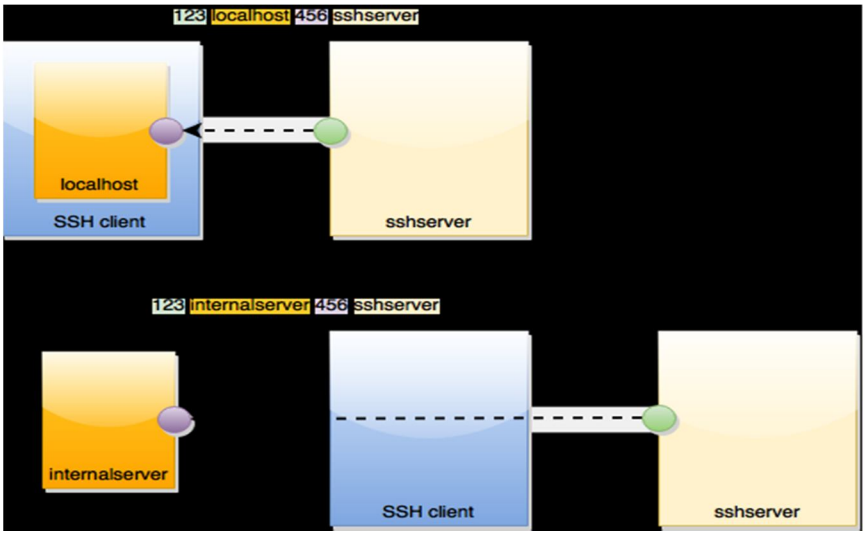


Figure: 3 Remote ports forwarding with Ssh via command line.

3) *Data Origin Authentication And Data Integrity:* To verify that the data sent on the VPN connection originated at the other end of the connection and was not modified in transit, the data contains a cryptographic checksum based on an encryption key known only to the sender and the receiver. Data origin authentication and data integrity are only available for L2TP/IPSec connections.

D. Data Encryption

To ensure confidentiality of the data as it traverses the shared or public transit network, the data is encrypted by the sender and decrypted by the receiver. The encryption and decryption processes depend on both the sender and the receiver using a common encryption key.

Intercepted packets sent along the VPN connection in the transit network are unintelligible to anyone who does not have the common encryption key. The length of the encryption key is an important security parameter. You can use computational techniques to determine the encryption key. However, such techniques require more computing power and computational time as the encryption keys get larger. Therefore, it is important to use the largest possible key size to ensure data confidentiality.

IV. CONCLUSION

In this work, we described three key properties for net-work moving target defense. A novel mobile IPv6 based moving target defense strategy is designed to continuously change IP addresses such that attackers are difficult to find them. 1. Zero extra network delay 2.Zero packet loss 3. Scalable 4.Versatile

Signaling overhead: Each round of changing IP needs two message transmissions at each MN (BU and BA messages) with each being 158 bytes (using IPsec).

A novel network IPv6 based moving target defense strategy is designed to continuously change IP addresses such that attackers are difficult to find them. For each data packet, we have 24 bytes of overhead due to the use of IPsec (ES).

V. FUTURE WORK

A. As a part of future work, the following tasks would be performed,

1) Incorporate network ort hopping using dynamic port Address Translation and NAT as part of the randomization in addition to IP hopping to increase the attack complexity & cost. Such approach clouds decrease the attack surface to a considerable extent, even for sophisticated attack scenarios.

2) Optimize the IP hopping algorithm further by incorporating modern encryption methods.

3) Re-study the experiments with all different implementations and compare their performance and security.

4) Expand the tested to multiple substations and multiple control centers.

5) The VPN network vulnerability in to addressing scheme-the fixed binding between hosts and IP address, which has been used by attacks to easily locate their victims.

REFERENCES

[1] Heydari, S. Kim, and S.M. Yoo, "Scalable Anti-Censorship Framework Using Moving Target Defense for Web Servers," IEEE Transactions on Information Forensics and Security, vol. 12, no. 5, May 2017, pp. 1113-1124. (pdf)

[2] V. Heydari and S.M. Yoo, "E2EACK: An end-to-end acknowledgment-based scheme against collusion black hole and slander attacks in MANETs," Springer's Wireless Networks, vol. 22, issue 7, Oct. 2016, pp. 2259-2273. (pdf)

[3] J. Gupta, E. Kalaimannan, and S.M. Yoo, "Maximizing investigation effectiveness in digital forensic cases," A Heuristic for maximizing investigation effectiveness of digital forensic cases involving multiple investigators," Computers & Operations Research, vol. 69, May 2016, pp. 1-9. (Pdf)

[4] V. Heydari and S.M. Yoo, "Lightweight acknowledgement-based method to detect misbehavior in MANETs," KSII Transactions on Internet and Information Systems, vol. 9, no. 12, Dec. 2015, pp. 5150-5169. (pdf)

[5] S. Park and S.M. Yoo, "Extended self-reproducible discrete event system specification (DEVS) formalism using hidden inheritance," Information Sciences, vol. 292, pp. 75-94, Jan. 2015. (pdf)

[6] Y. An, S.M. Yoo, C. An, and B.E. Wells, "Rule-based multiple-target tracking in acoustic wireless sensor networks," Computer Communications, vol. 51, pp. 81-94, Sep. 2014. (pdf).

[7] M. Avula, S.G. Lee, and S.M. Yoo, "Security framework for hybrid wireless mesh protocol in wireless mesh networks," KSII Transactions on Internet and Information Systems, vol. 8, no. 6, pp. 1982-2004, June 2014. (pdf).

[8] W.K. Tan, S.G. Lee, J.H. Lam, and S.M. Yoo,"A security analysis of the 802.11s wireless mesh network routing protocol and its secure routing protocols," (MPDI) Sensors 13(9), pp. 11553-11585, Sep. 2013. (pdf)

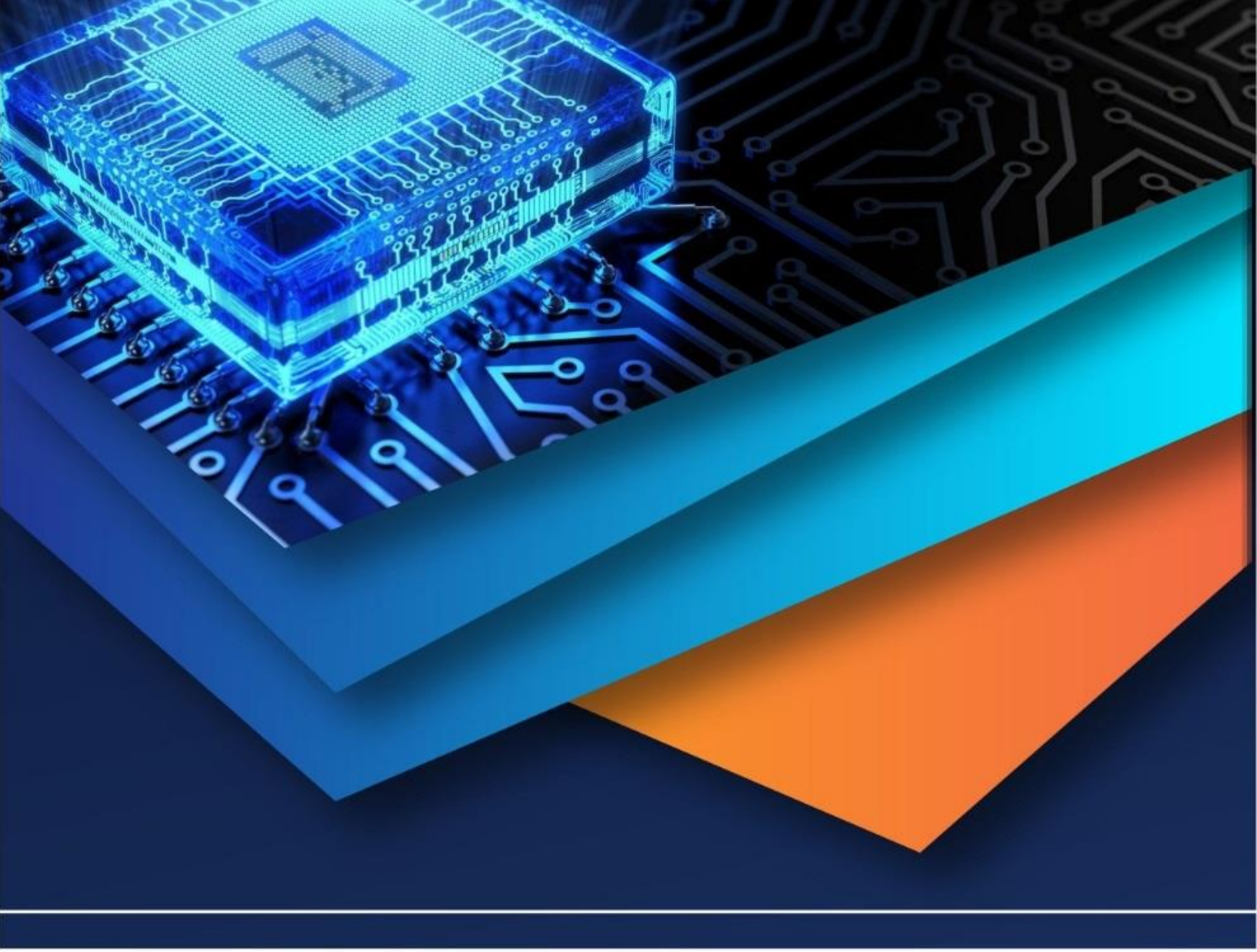
[9] Y. An, S.M. Yoo, C. An, and B.E. Wells, "Noise Mitigation for Target Tracking in Wireless Acoustic Sensor Networks," KSII Transactions on Internet and Information Systems, vol. 7, no. 5, pp. 1166-1179, May 2013. (pdf)

[10] Y. An, S.M. Yoo, C. An, and B.E. Wells, "Doppler effect on target tracking in wireless sensor networks," Computer Communications, vol. 36, issue 7, pp. 834-848, Apr. 2013. (pdf) 11. S. Park and S.M. Yoo, "An efficient reliable one-hop broadcast in mobile ad hoc networks," Ad Hoc Networks, vol.

[11] issue 1, pp. 19-28, Jan. 2013. (Pdf)

[12] M. Avula and S.M. Yoo, "An energy-efficient minimum connected dominating set in mobile ad hoc networks," Int'l Journal of Ubiquitous Computing and Internationalization, vol. 4, no. 1, pp. 25-28, Dec. 2012 (pdf).

[13] J.C. Lee and S.M. Yoo, "Intelligent cell selection satisfying user requirements for intersystem handover in heterogeneous networks," Computer Communications, vol. 35, issue 17, pp. 2106-2114, Oct. 2012. (Pdf)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY