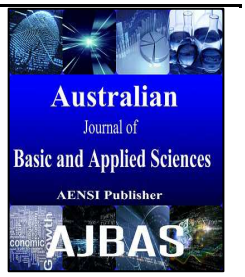
Australian Journal of Basic and Applied Sciences, 9(35) November 2015, Pages: 218-224

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com



An Extended Hybrid Intrusion Detection & Prevention System for Distributed Network

[1]A. Thomas Paul Roy and [2]Dr.K. Balasubadra

[1]*Assistant Professor, Department of CSE, PSNA College of Engineering and Technology, Dindigul, India.*
[2]*Professor, Dept. of CSE., R.M.D. Engineering College, Kavaraipettai, Tiruvallur Dt., Tamil Nadu – 601 206, India.*

ARTICLE INFO

Article history:
Received 10 October 2015
Accepted 30 November 2015
Available online 24 December 2015

Keywords:
MANET, Security, Intrusion, Anomaly, Signature.

ABSTRACT

In the Earlier research work provides a Hybrid Intrusion Detection and prevention System (HIDS) where the malicious nodes are detected anomaly by broadcasting block messages to other nodes in the network. So that, the other node can isolates the malicious nodes from the basic communication and prevent the network functionality. Detecting the malicious in the existing system is obtained by verifying the properties and signature of the nodes. The existing system focused on Black-Hole, Flooding and Rushing attacks. But the proposed system extends the HIDS and includes some more functionality to detect any type of malicious activities in the network. EHIDS provides three major operations such as Authentication and Authorization for investigating the nodes, signature verification for investigating the data and Data-integrity for data maintenance. Since, EHIDS can checks malicious activities on the route, other side of the route and entire network. These techniques employ ns2 to validate the effectiveness of Intrusion Detection system and EHIDS proved it is better approach than the HIDS.

© 2015 AENSI Publisher All rights reserved.

ToCite ThisArticle:A. Thomas Paul Roy, An Extended Hybrid Intrusion Detection & Prevention System for Distributed ***Aust. J. Basic & Appl. Sci.,*** *9(35): 218-224, 2015*

INTRODUCTION

In a wireless Mobile Ad hoc Network (MANET), there are no routers or access points; data transfer among nodes is achieved by means of multiple hops. Every mobile node acts both as a host and as a router to establish a route. When a source node tries to transfer data to a destination node, packets are forwarded through the intermediate nodes, thus, searching for and immediately establishing a route from a source to a destination node is an important is an important issue for MANETs. In a reactive routing protocol such as AODV (Ad hoc On-Demand Distance Vector) or DSR (Dynamic Source Routing), a route is searched and established only when two nodes intend to transfer data. Because most of these routing protocols assume cooperation between nodes for packet forwarding, a malicious node can launch routing attacks that disrupts the normal routing operations or Denial-Of-Service (DOS) attacks such as black hole or gray-hole attack that denies the service to the legitimate nodes on MANET.

MANETs are generally used for communication during natural hazards, on the battlefield, and business communications. So data transfer between two nodes requires security. Most secure routing protocol is designed to prevent hazards to safety properties, such as: (1) authentication and non-repudiation; (2) availability of resources; (3) integrity; and (4) confidentiality and privacy. These security mechanisms can prevent only external attacks, i.e., attacks launched by external nodes that do not belong to the network. However internal attacks (Kejun Liu, *et al*., 2007) such as black hole or gray-hole attack, routing attacks and worm-hole attacks are very hard to detect, because it is launched by compromised nodes that have been authorized by the victim network.

In Black hole attack, a malicious node can attract all data packets by falsely claiming a fresh route or shortest route to the destination and then absorbs them without forwarding it to the destination. Flooding is a Denial of Service (DoS) attack that is designed to bring a network or service down by flooding it with large amounts of traffic. Flooding attacks happens when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests. Rushing attacks which are result in denial of services. Rushing attack exploits this duplicate suppression mechanism by quickly forwarding route discovery packet in order to gain access to the forwarding group. When a node send a route request packet (RR packet) to another node in the wireless network, an attacker present in

Corresponding Author: A. Thomas Paul Roy, Assistant Professor, Dept. of CSE., P.S.N.A. College of Engineering and Technology Dindigul-624 622, TamilNadu, India.
E-mail: pauli.dgl@gmail.com

the network will accept the RR packet and send to his neighbor with high transmission speed as compared to other nodes, which are present in the wireless network. Due to this high transmission speed, packet forwarded by the attacker will first reach to the destination node. Destination node accepts this RR packet and discards other RR.

Related Works:

Black hole, Flooding & Rushing attacks are regarded as Network Layer Attacks and they have serious impact on reactive routing protocols such as AODV (Abolhasan Mehran, Wysocki Tadeuz, 2004) or DSR (Johnson, D.B., *et al*., 2004). In (Hidehisa Nakayama, Satoshi Kurosawa, 2009) Anomaly-detection scheme using AODV based Routing Scheme is Proposed its having a Disadvantage of High false Alarm Rate. In (Balachadran, S., *et al*, 2010) A Hybrid approach is proposed, using DSR Protocol for MANET for Misbehavior detection among mobile nodes, having some limitations include, not scalable to large network and requires more processing resources. In (Mohanapriya, M. Ilango Krishnamurthi, 2013) a survey of routing protocols is described and it is found that AODV Protocol is highly scalable, it finds the least congested route instead of shortest path, no additional overheads and Quickly Responsive. Kejun Liu *et al* (2007) and S.N.Chobe (2013) proposed the 2ACK method where it helps to detect the intruder node in terms of misbehavior. 2ACK analyzes the acknowledgement packet by their request and response messages. Jakobsson, M. and Hubaux (2003) said the idea of nuggets is used as payment. There are twoprototypes1) Packet trade type 2) Packet purse type. In the Packet Trade type, each in-between node purchases the packet from the earlier node for some nuggets and retails it to the following node for more nuggets Jakobsson, M. and Hubaux (2003).

From the above discussion about the malicious detection using various approaches they find partial solutions. Hence, it is motivated to develop a novel approach which can provide a complete solution for detecting and preventing malicious activities. In this paper an extended hybrid IDS model is designed and EHIDS to fulfill the requirement for wireless sensor networks.

Existing Approach:

The existing IDS model (Mithun, S and A. Thomas Paul Roy, 2015) is based on the following algorithms & Techniques. The System using Anomaly, based on Algorithms which detects malicious nodes in the network. This Anomaly based techniques having a Disadvantage of High False Alarm Rate, so adding a Signature based methodology will rectify this and gives more Accuracy in Fault node detection. Fig.1 shows the overall architecture for Hybrid Intrusion Detection & Prevention System using Hybrid technique. The System maintains a Database which contains two tables, the first table contains information about Node number and their malicious behavior, Second table contains Prevented Node Information that recently reported anomalies. The System starts by inputting Nodes information that participates in routing, and then the Anomaly Detection Engine checks the nodes being participated had reported any anomalies in recent past. If so it avoids those nodes from routing. After that A Modified AODV protocol is used to check whether newly participating nodes having any anomalous behavior, if any anomalous behavior is detected the information is passed to Signature Engine it will cross check the database for corresponding node id, if node id is recorded as a recent past attack those nodes will be avoided from routing.

Extended Hybrid Intrusion Detection System:

EHIDS do its functionality in three stages such as (i). Authentication and Authorization, (ii). Signature Verification and (iii). Data Integrity. Nodes are assigned by a unique name when it is created. During communication such as route discovery and data transmission the participant nodes are authorized in terms of their unique name only. The node unique name is generating and assigning node number in term of its region and its serial number. The region ID indicates the region number, and M numbers of nodes are deployed in region wise, randomly within the region, where the number of nodes in each region is equal. During node creation, BS generates a 5 digit number as NID and assign to each node in the network. For example the node N_3 receives the NID as:

NID for N_3 is "000 63 3"

Where 000 is the starting number, 63 is randomly generated by $RANDBETWEE\ (0, 100)$ and 3 is the region number, where N_3 is placed in region-3. Likewise, all the nodes in the network are assigned by a uniqueNID , where; it helps for identifying the nodes within the network. Similarly all the nodes are assigned by a private and public key for providing security for their data. Signature verification is done by applying a public and private key to the entire nodes for dynamic verification and data encryption decryption while data transmission. The public and private key is given from the location of each node in the network. Each node is deployed in a dynamic location (x, y) where the location value is the key for the node and it can be represented as:

$$Ni_{key} = key(node_i) = node_i(x_i, y_i) \quad \text{---}$$

Equation [1]

For data communication, a node is required to submit its key pair; if the key value is valid, the node

is allowed to communicate with other nodes; otherwise the node is blocked from communication. It is discussed that the proposed approach considers the distance among the source and destination nodes. It is well known that the time taken to transmit a data from source to destination is few milli seconds for short distance. And for long distance it takes little more time than the short distance. EHIDS assumes that, within a short distance transmitting the data packet is safe and secure. Data security is considered only for long distance based data transmission. The encryption and decryption functionality is also too simple and easy to code for reducing the computational complexity and fast execution.

Procedure String Encrypt (String D[ ], String Ni_key):

```
{
    String plaintext[ ]  = D;
    Chiphertext Ct [ ] = (plaintext + Ni_key);
        return Ct;
}
```

Procedure String Decrypt (String Ct[ ], String Ni_key):

```
{
    String Chiphertext[ ]  = Ct;
    plaintext pt [ ] = (Chiphertext - Ni_key);
        return pt;
}
```

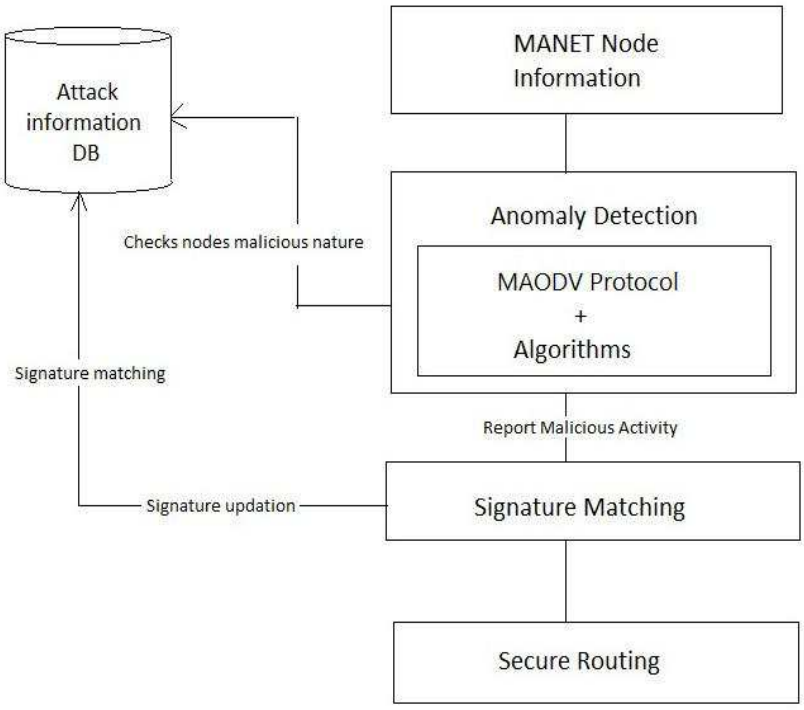


Fig. 1: Hybrid Intrusion Detection System

By adding and removing the node key into the plaintext and the chiphertext provides encrypted and decrypted data respectively. The above procedures help to code in any simulator to verify the performance of the optional cryptography mechanism.

Finally during data transmission the source node and the destination node are verified with their NID before going to start routing. After routing, a path is selected among the source and destination nodes then finally the destination node is verified once again by comparing its NID and the Ni_{Key} from itself and with BS and with neighboring nodes in the network. If all the information is similar then only the data will passed to destination. Our proposed approach provides better efficiency in terms of authenticating the nodes, verifying the destination node and secured transmission. In case of BS wants to send the aggregated data to relevant node, data and the node authentication is verified once again for data integrity. The data integrity helps to achieve the data delivery only to the data-owner. Data integrity always provides the data only to the owner after verification of the node identity, and node key and other relevant information.

Simulation Settings:

The proposed approach is simulated in Network Simulator-2 and the parameters assigned for the simulation is given in the following Table-1. All other parameters take default value.

Australian Journal of Basic and Applied Sciences, 9(35) November 2015, Pages: 218-224

Table 1: Parameter Settings in NS2

Parameters	Value
Area	1000m x 1000m
Speed	1 to 15 m/s
Radio Propagation Model	Two-ray ground reflection
Radio Range	250 m
Number of Nodes	100 to 1000
MAC	802.11
Application	CBR, 100 to 500
Packet Size	50
Simulation Time	100 s
Node Deployment	Random
Maliciou Population Generation	Up to 5%

To prove the efficiency of the EHIDS, the entire functionality is simulated in Networks Simulator software. The area size is 1000 x 1000, where the number of nodes deployed is from 100 to 100 in numbers. To verify the performance more number of iteration is applied in the simulation with various numbers of nodes deployed in the network. The front end of the simulation is written in TCL and backend coding is done in .cc code. The Figure-5 shows that the network is deployed with 100 nodes and how the nodes are named and communicate with each other. During the communication EHIDS functionality is defined and malicious node is also detected by checking the DP of each node participate in the network function. It is assumed all the nodes function under IEEE 802.11 standard. An amount of energy can be reduced from the current- energy level of the node.

RESULTS AND DISCUSSION

The existing system verifies only few threats occur in the network. Ratio of the total number of data packets dropped by the malicious nodes and also due to congestion to the total number of data packets sent. AODV having high Packet Overhead because in addition to Route Discovery controls it using Sequence messages. If the source route is without any malicious nodes, then the end-to-end delay for transmitting data packets is less because, there is no additional overhead of checking for presence of attackers. Here we demonstrated all protocols with initial attack conditions. The entire performance of the EHIDS is depicted in terms of Packet Delivery, control packet overhead and end-to-end delay.

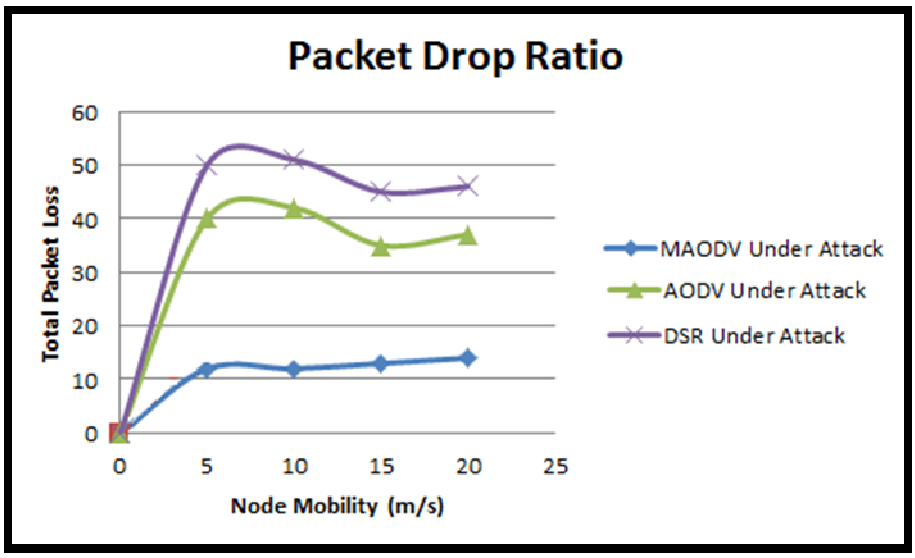


Fig. 2: HIDS Performance in terms of Packet Delivery Ratio

Australian Journal of Basic and Applied Sciences, 9(35) November 2015, Pages: 218-224

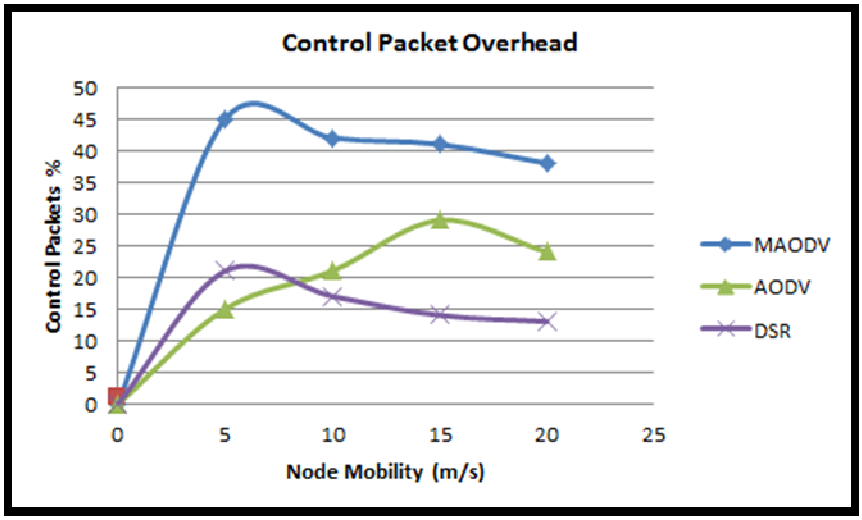


Fig. 3: HIDS Performance in terms of Control Overhead

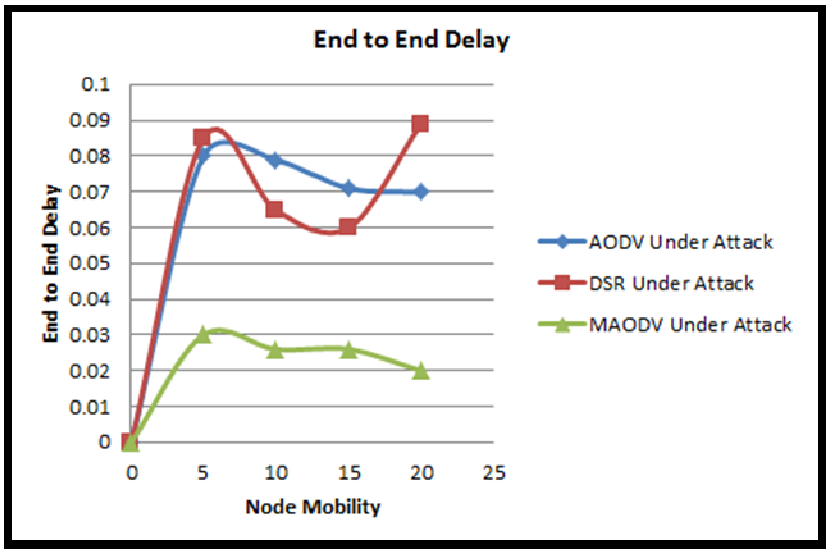


Fig. 4: HIDS Performance in Terms of End-to-End Delay

In the simulation, 100, 200, 500, 1500 and 2000 number of nodes are deployed in the network and the functionality is verified. Initially the number malicious nodes are detected by verifying the Node-ID of the node who participates in the data transmission. To check the performance the simulation is applied two time one is without HIDS [existing approach] and the other one is with EHIDS [proposed approach].

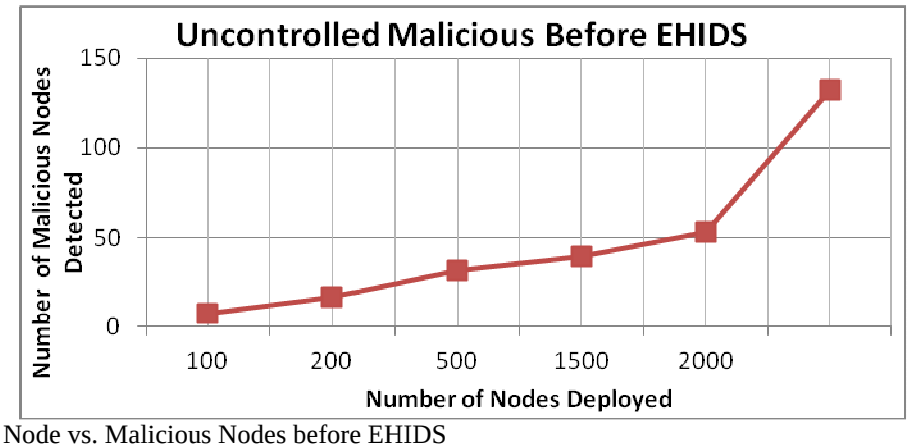


Fig. 5: Normal Node vs. Malicious Nodes before EHIDS

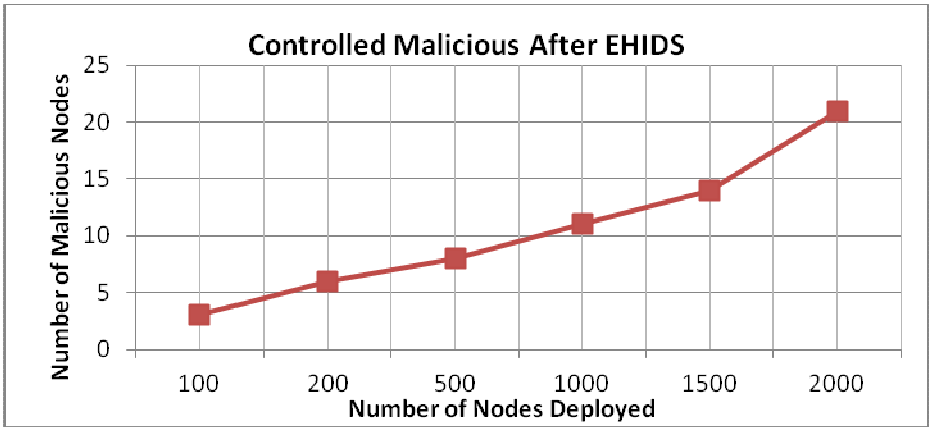


Fig. 6: Normal Node vs. Malicious Nodes after EHIDS

The result is shown in Figure-5 illustrates the malicious behavior before deploying EHIDS in the network. The number of malicious activity is increased according the number of nodes deployed in the network. From figure-5, it is clear and can understand that for more number of nodes number malicious activity found and for less number of nodes less number malicious activity found. Figure-6 shows the controlled malicious activity by EHIDS and it illustrates that, while verifying the node information itself they are eliminated and not reoccur during data transmission.

Conclusion:

The main objective of this paper is to design and develop a novel framework for intrusion detection in wireless sensor network. To fill that an EHIDS is developed and it functions in three levels. In all the three level, EHIDS tights the security and provide a better secured data transmission by detecting and eliminating malicious nodes in the network. From the simulation results EHIDS controls the malicious activity and it is proved through the graph. In future EHIDS can be extended by including confidentiality, data integrity and other function which makes more security in the network.

REFERENCES

Abolhasan Mehran, Wysocki Tadeuz, 2004. ”A review of routing protocols for mobile ad hoc networks”, Int J Ad hoc Networks, 2(1): 1-22.

Balachadran, S., D. Dasgupta, L. Wang, 2010. “A Hybrid Approach for Misbehavior Detection in Wireless Ad-hoc Networks”. Sunil Taneja, Ashwani Kush International Journal of Innovation.

Chobe, S.N., DeepaliGothawal, 2013. “An Acknowledgement Based Approach For Routing Misbehavior Detection In MANET With AOMDV”, Proceedings of International Joint Conference, Goa, India, ISBN: 978-81-927147-7-6.

Hidehisa Nakayama, Satoshi Kurosawa, 2009. “A Dynamic Anomaly Detection scheme for AODV-Based Mobile Ad-hoc Networks”, IEEE.

Jakobsson, M. and J.P. Hubaux, and Butty, 2003. “A micro-payment scheme encouraging collaboration in multi-hop cellular networks”, Computer Aided Verification, pages=15–33, year=2003, organization= Springer.

Johnson, D.B., D.A. Maltz, Y-C. Hu, 2004. “The dynamic source routing protocol for mobile ad-hoc network (DSR)”, IETF Internet Draft.

Kejun Liu, Jing Deng, Member, IEEE, Pramod K. Varshney,Fellow, IEEE and Kashyap Balakrishnan, Member, IEEE, 2007. “An Acknowledgment-Based Approach for the Detection of Routing Misbehaviour in MANETs”, IEEE Transactions on mobile computing, 6(5).

Mithun, S and A. Thomas Paul Roy, 2015. “A Hybrid Intrusion Detection & Prevention System in A Distributed Network”, International Journal of Applied Engineering Research, ISSN 0973-4562, 10: 20.

Mohanapriya, M. Ilango Krishnamurthi, 2013. “Modified DSR protocol for detection and removal of selective black hole attack in MANET” , Elsevier.

Semih Dokurer, Erten Y.M., Can Erkin Acar, 2007 ”Performance analysis of ad-hoc networks under black hole attacks”, In: Proc. of the IEEE South East Con, pp: 148-53.

Thomas Paul Roy A. & K. Balasubadra, “DAD: A Secured Routing Protocol for Detecting and Preventing Denial-of-Service in Wireless Networks”, Wireless Personal Communication, DOI 10.1007/s11277-015-3022.