Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2017) 25: 2761 – 2769

doi:10.3906/elk-1508-121

A secure cross-layer AODV routing method to detect and isolate (SCLARDI) black hole attacks for MANET

Usha GOPAL[1,*], **Kannimuthu SUBRAMANIAN**[2]
[1]Information Technology, Karpagam College of Engineering, Coimbatore, India
[2]Computer Science and Engineering, Karpagam College of Engineering, Coimbatore, India

Received: 14.08.2015 • **Accepted/Published Online:** 31.10.2016 • **Final Version:** 30.07.2017

Abstract: In this paper, a secure cross-layer–based routing technique (SCLARDI) for a mobile ad hoc network (MANET) is proposed. This technique makes use of ad hoc on-demand routing protocol (AODV) algorithms and honeypot technology to detect and isolate black hole attacks from MANETs. This novel system is compared with the single-layer design techniques and existing cross-layer detection techniques. Out of the tested models, the proposed cross-layer design is the most suitable for MANET security. First, the vulnerabilities of the AODV routing protocol against black hole attacks are analyzed. Second, a secure cross-layer–based AODV routing technique is proposed. The proposed SCLARDI technique detects and isolates black hole attacks from MANET. Finally, the results are compared with the existing techniques. The simulations are done using NS-2. The simulation results show that the proposed technique improves the packet delivery ratio and reduces network overhead, normalized routing load, and packet drop ratio compared to other existing single-layer and cross-layer techniques.

Key words: Ad hoc on-demand routing protocol, black hole attacks, cross layer, mobile ad hoc network, packet delivery ratio

1. Introduction

A mobile ad hoc network (MANET) consists of dynamic, self-configuring, and self-deployable nodes, where each node acts as a router. Unlike cellular or wired networks, MANETs do not require any base station or centralized routers, due to their ad hoc nature. Initially, the routing protocols in MANET are not designed to secure against malicious attackers. The routing protocol designers only consider routing between the nodes. Routing algorithms used nowadays are not designed to handle attackers [1,2]. Protocol designers assume that the MANET environment is trusted and cooperative; as a result, security is not considered [3,4]. In a MANET, unlike a wired network, mobile nodes roam here and there. Thus, strictly layered architecture is not sufficient to deal with the dynamics of a wireless network environment. MANET security cannot be solved by isolating a single layer [5]. Hence, this paper uses a cross-layer security technique that enhances the network performance of MANET by exchanging or sharing information between the layers [6–8]. Recently, a lot of new cross-layer design techniques have been proposed to improve the performance of MANETs [9,10]. Before understanding cross-layer design, the most vulnerable behavior of the black hole attack in an ad hoc on-demand (AODV) routing protocol is discussed.

*Correspondence: ushag2@gmail.com

1.1. Black hole attack in AODV

A black hole attack is a type of DoS attack. It is a severe threat against a routing protocol accomplished by dropping packets. The AODV routing protocol suffers from various types of security problems. The main aim of the black hole attack is to make the destination node unreachable or downgrade communication throughout the network. The invisible act of black hole nodes can be detected by only monitoring the lost traffic. A black hole attacker drops all the packets in a communication path. The AODV routing protocol is used in this paper because it has a lot of vulnerabilities. Next, the importance of cross-layer design and security is discussed.

1.2. Cross-layer security

Cross-layer design exploits dependencies between the layers, which increases performance. Cross-layer design shares knowledge about the state and conditions of one layer to the other layers. In cross-layer designs, not all layers need to be coordinated or optimized jointly. In this work, the MAC and routing layer layers are considered. In order to improve security, these two layers are considered with minimum features. If the features are minimal, the network processing overhead is reduced. In addition to cross-layer security, a honeypot-based security technique is also discussed in this work. A honeypot provides precise information with a very small amount of data that contains malicious activity. Next, an overview of the honeypot security technique is discussed.

1.3. Honeypot security

Spitzner defined a honeypot as a "security resource, whose value is probed, attacked or compromised." A honeypot is a computing resource that is closely monitored in order to be intruded, attacked, or compromised. The proposed secure cross-layer–based routing security solution (SCLARDI) includes a honeypot-based detection and isolation technique for MANETs. Most existing black hole detection techniques use only single-layer detection techniques. However, an adversary may launch various types of attacks targeting multiple layers. Hence in this paper, a cross-layer–based technique that uses the honeypot concept is discussed.

The remainder of this paper is structured as follows. Section 2 presents related work in the areas of honeypot security and cross-layer security. Section 3 describes the proposed SCLARDI methodology. Section 4 discusses the simulation results. Finally, Section 5 concludes the paper.

2. Related work

Various authors have proposed security solutions to protect MANETs from attacks [11,12]. Honeypots are a special type of mechanism for intrusion detection, designed to trap attackers and gather information about them. Honeypots are used in cluster-based MANETs [13]. Physical-media–independent architecture [14] is used to pass information to upper layers about changes at the network interface. In their proposed technique, a mobile computer adapts itself dynamically. A set of device characteristics is defined and the interlayer signaling pipe [15] is used to store cross-layer information in the wireless extension header.

A cross-layer technique is proposed in [16] to defend against black hole attacks in MANETs using CARDS. It utilizes machine learning algorithms to defend against security problems in MANETs. Their technique consists of three modules: data collection, data reduction, and learning. A shared database model [17] is proposed to detect attacks in MANETs. They propose two types of architecture, Type I cross-layer IDS (CIDS) and Type II CIDS.

3. Proposed SCLARDI methodology

Figure 1 illustrates the proposed SCLARDI architecture for MANETs. The proposed SCLARDI architecture consists of the following main components:

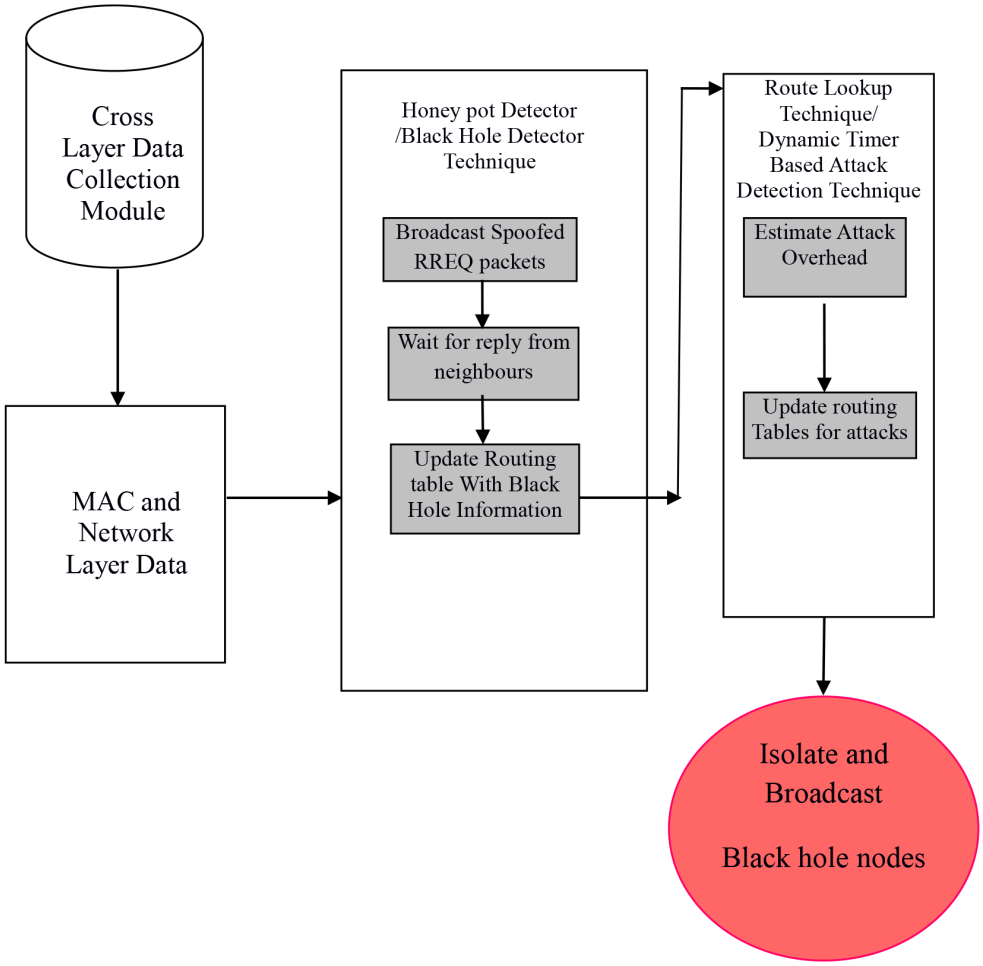

Figure 1. Proposed SCLARDI architecture.

1. Black hole detector/honeypot detector
2. Route lookup in cross layer

3.1. Black hole detector/honeypot detector

The honeypot detector module is responsible for detecting black hole nodes in the network. To begin with, the honeypot detector initializes the malicious node detection process. First, it broadcasts spoofed RREQ packets. The spoofed RREQ packets contain a nonexistent source ID and a TTL value set to 1. This RREQ packet is known as a spoofed RREQ/honeypot detector packet. Then this spoofed RREQ packet is broadcasted to all other nodes in the network. The broadcasted honeypot-spoofed RREQ packet waits for a reply from the neighbor nodes. If any neighbors reply to this packet, those nodes are marked as black hole nodes in the routing table. Normal nodes, which are not malicious, do not reply to this spoofed RREQ packet because the spoofed

packets generated by the honeypot node contain a nonexistent source ID. Hence, the routing table updates this black hole node information by marking it as a malicious node. The algorithm for the malicious node detection timer function is given below. This function also invokes SendSpoofedRouteRequest(), which broadcasts the spoofed RREQ messages to neighboring nodes in the network. This algorithm creates a nonexistent IP address by checking the routing table entry and then adds the nonexistent routing address to the routing table. Then it broadcasts the spoofed RREQ packet to all the nodes in the network. Additionally, it calls for another function, which originally sends the fake request to all the nodes in the MANET. The following algorithm is responsible for malicious node detection when the algorithm sends spoofed RREQ packets.

Algorithm for Malicious Node Detection

```
    Input      : Routing layer Data
    Output     : Malicious RREQ Data
Function : MaliciousNodeDetectionTimer ( )
Begin
    SendSpoofedRouteRequest ();
End.
```

The above MaliciousNodeDetectionTimer() algorithm is used to send spoofed RREQ packets throughout the network. Since the above algorithm uses a recursive function, it invokes the following SendSpoofedRouteRequest() algorithm to send fake RREQ messages throughout the network.

Algorithm for sending spoofed RREQ

```
Function SendSpoofedRouteRequest ()
Begin
   aodv_rt_entry *rt;
// Create a nonexisting IP address
   NEAddress ← NonExistingNodeID;
   Rt ← rtable.rt_lookup (NEAddress);
   if (rt == 0)
         rt ← rtable.rt_add (NEAddress);
   SendFakeRequest (NEAddress);
End
```

The honeypot node assigns a nonexistent node ID to a particular network. Next, this new nonexistent node ID is added to the routing table. The variable rt is used to assign the nonexistent node ID. By using this nonexistent node ID, the spoofed packets are broadcasted throughout the network. The algorithm steps for sending fake requests are given below:

3.2. Algorithm for sending fake requests

The below algorithm broadcasts a fake request. In an AODV RREQ packet, it fills the spoofed TTL value and wrong node address. In this way, the fake RREQ packets are broadcasted throughout the network by the honeypot node.

```
Function SendFakeRequest (NEAddress)
    Begin
    // allocate a RREQ packet
        SpoofedRREQ_Packet Create_Default_RREQ_Packet ()
    // Fill out the RREQ packet with Spoofed Info
        SpoofedRREQ_Packet -> rq_TTL = 1;
        SpoofedRREQ_Packet -> dst = NEAddress;
        Broadcast (SpoofedRREQ_Packet);
    End
```

3.3. Modified route lookup in cross layer

Route lookup in the cross layer is responsible for dynamically invoking the detection process based on the attack load. Whenever the attack load increases, the dynamic timer technique starts the detection process. The following algorithm illustrates the dynamic timer algorithm that initiates the timer technique.

```
Algorithm
    Input: Check Attack load data
    Output: Invoke the timer based on the attack load
Function Timer ( )
Begin
    if (EstimatedAttackLoad <= LoadStep)
        EstimatedAttackLoad = Load Step
    else
        EstimatedAttackLoad = EstimatedAttackLoad + Load Step;
    if (EstimatedAttackLoad > MaxAllowedLoad)
        EstimatedAttackLoad = MaxAllowedLoad
    else
        EstimatedAttackLoad = EstimatedAttackLoad;
    End
```

The above algorithm is responsible for detecting any attack load from the network. If the black hole attack load is great, this algorithm invokes the detection process dynamically. Hence, the proposed technique reduces the overhead of the network. Additionally, the cross-layer features used in this technique improve network performance.

4. Performance evaluation

In order to evaluate this SCLARDI technique, various performance metrics were used. Packet delivery fraction (PDF) is a useful metric for measuring how many packets are delivered from the source node to the destination node. Normalized routing load (NRL) is used to measure the network load caused by control packets. End-to-end delay (EED) is a useful metric for calculating the delay. Packet drop ratio is used to determine the causes of packet loss in the network. Table 1 illustrates the simulation environment for the proposed technique. The simulation environment, traffic parameters, and variable parameters were used for the SCLARDI technique.

Table 1. Simulation environment.

Parameters	Values
Channel type	Wireless channel
Radio propagation model	Two-ray ground model
Antenna type	Omni antenna
Interface queue type	Drop Tail/Pri Queue
MAC type	802.11
Maximum packet in queue	50
Topographical area	600×600 m^2
Mobility scenario	10 m/s
Pause time	20 s
Mobility model	Random waypoint model

The parameters in Table 2 were used as the traffic parameters. The parameters in Table 3 were used as the variable parameters. For each set of parameters, the simulations were repeated 3 times and the average of the results was calculated. The following experiments were conducted in order to demonstrate the improvement of the proposed SCLARDI technique.

Table 2. Traffic parameters.

Parameters	Values
Traffic agent	CBR
Transport agent	UDP
Traffic source	7
CBR rate	10 kbps

Table 3. Variable parameters.

Parameters	Values
Routing protocols	Normal AODV
AODV with black holes	1, 2, 3, and 4
Number of nodes	20

a. Normal AODV
b. AODV without any detection and black hole attacks
c. AODV with the proposed SCLARDI technique
d. Comparison of the proposed technique with the existing techniques

The SCLARDI technique was compared with both the AODV and single-layer techniques. In each comparison, the proposed SCLARDI technique performs considerably better than the existing AODV and single-layer techniques. As seen in Table 4, the SCLARDI technique performed better than the other existing techniques, where a comparison corresponding to PDF values when 40% of the network consists of malicious nodes. In SCLARDI, the detection process is invoked dynamically by considering the attack load of the MANET. PDF is 92.87% for the proposed SCLARDI technique when 10% of the network consists of black hole nodes. The existing single-layer technique PDF is 89.03% and for AODV it is 67.73% under the same conditions. As seen in Figure 2, the proposed SCLARDI technique drops 150 packets/s when 10% of the network consists

of black hole nodes. The single-layer technique drops 229 packets/s and the existing AODV algorithm drops 590 packets/s under the same conditions, as shown in Figure 3. Hence the proposed SCLARDI technique performs considerably better than the normal AODV and single-layer techniques. From Figure 4, the following observations are made for NRL. In the proposed technique, NRL is measured in terms of kbps. Without a detection technique, NRL increases slightly when 30% of the network consists of black hole nodes. After that, NRL increases exponentially when the system uses no detection technique. The proposed detection technique

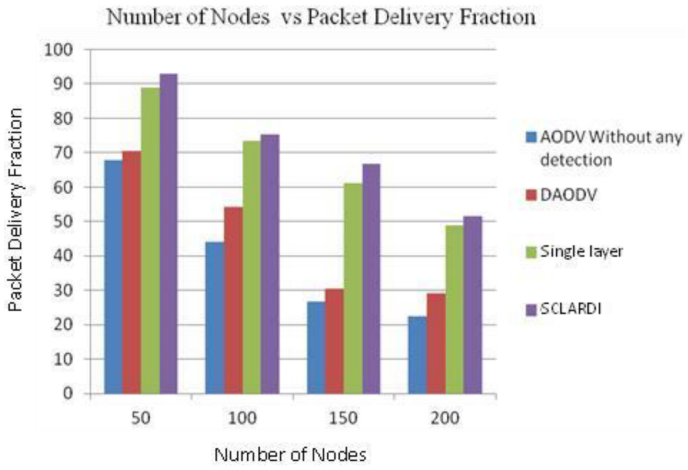

Figure 2. Comparison of the packet delivery fraction.

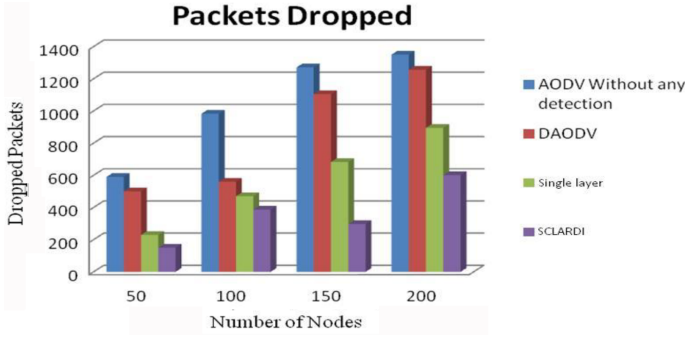

Figure 3. Comparison of dropped packets.

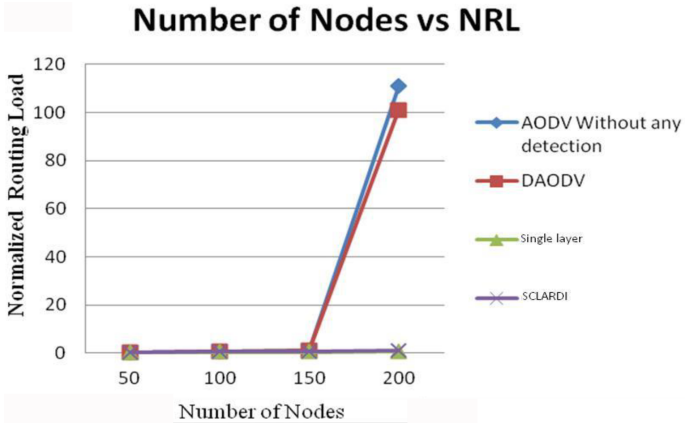

Figure 4. Comparison of the normalized routing load.

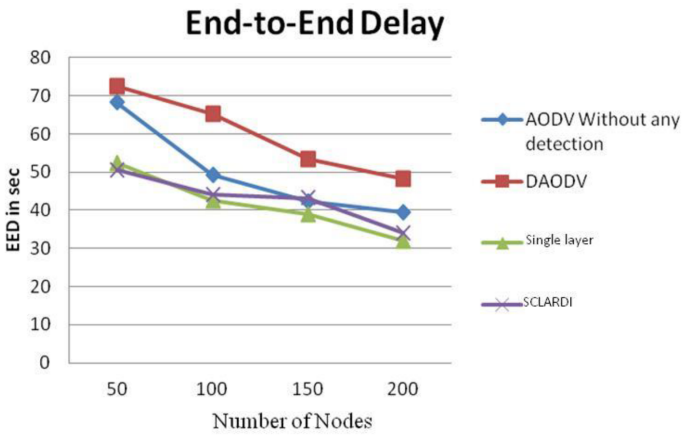

Figure 5. Comparison of the end-to-end delay.

implements the SCLARDI technique, and hence there is a reduction in the NRL, as in Figure 4. Thus, the NRL is reduced for the proposed SCLARDI technique. EED decreases when the percentage of malicious nodes increases. In the proposed SCLARDI technique, EED decreases significantly, which indicates that the connection is established within the lower number of hops, as shown in Figure 5. That is, when there is a malicious node in the network, the proposed SCLARDI technique detects and isolates it from the network. Hence, communication is only via the normal nodes and so EED is decreased. PDF is 92.87% for the proposed SCLARDI technique when 10% of the network consists of black hole nodes. In the existing single-layer technique, PDF is 89.03% and for AODV it is 67.73% under the same conditions. Hence the proposed SCLARDI technique performs considerably better than the normal AODV and single-layer detection techniques. In the proposed SCLARDI technique, EED decreases significantly, which indicates that the connection is established within the lower number of hops. When there is a malicious node in the network, the proposed SCLARDI technique detects and isolates it from the network. Hence, communication is only via the normal nodes and so EED is decreased. The proposed cross-layer work is compared with the existing AODV technique, AODV protocol, and the single-layer technique. The proposed cross layer technique improves the PDF compared to the other existing techniques, as shown in Table 4.

Table 4. AODV with the proposed SCLARDI cross-layer technique.

Black hole node	PDF	NRL	EED	Routed packets	Dropped
1	92.87	0.43	50.59	722.67	150
2	75.23	0.70	44.10	717.33	387
3	66.73	0.82	43.17	740.00	297
4	51.67	1.11	34.07	756.33	601

5. Conclusion

In this paper, SCLARDI has been proposed. Extensive experimental investigations confirm that SCLARDI is superior to the AODV and single-layer techniques. PDF is improved in the proposed SCLARDI technique to 92.87%, which signifies an improvement in PDF. NRL is reduced in the proposed technique to 1.11 kbps, while for the existing AODV protocol NRL is 110.79 kbps. This shows that the network overhead is reduced in the proposed SCLARDI technique. EED is reduced to 50.59 s using the proposed SCLARDI technique. With the SLBHAD technique, EED is 52.37 s and for the existing AODV technique it is 68.24 s. EED is reduced

in the proposed SCLARDI technique. When 40% of the network consists of malicious black hole nodes, the routed packets are increased to 756 packets/s. The results demonstrate that the proposed SCLARDI technique improves PDF and routed packets, and reduces PDR, NRL, and EED.

References

[1] Agrawal P, Ghosh RK, Das SK. Cooperative black and gray hole attacks in MANETs. In: ACM 2008 Ubiquitous Information Management and Communication Conference; 31 January–1 February 2008; New York, NY, USA: ACM. pp. 310-314.

[2] Nasipuri A, Casaneda R, Das SR. On-demand multipath routing for MANETs. In: IEEE 1999 INFOCOM Conference; 11–13 October 1999; Boston, MA, USA: IEEE. pp. 64-70.

[3] Yi S, Kravets R. Composite key management for ad hoc networks. In: IEEE 2004 First Annual Mobile and Ubiquitous Systems Networking and Services Conference; 22–26 August 2004; Boston, MA, USA: IEEE. pp. 52-61.

[4] Qi W, Abu-Rgheff MA. Cross layer signalling for next generation wireless systems. In: IEEE 2003 Wireless Communications and Networking Conference; 16–20 March 2003; New Orleans, LA, USA: IEEE. pp. 1084-1089.

[5] Ning P, Sun K. How to misuse AODV: A case study of insider attacks against mobile ad hoc routing protocols. In: IEEE 2003 Fourth Annual Information Assurance Workshop; 18–20 June 2003; Raleigh, NC, USA: IEEE. pp. 60-67.

[6] Nadeem A, Howarth M. Protection of MANETs from a range of attacks using an intrusion detection and prevention system. Telecommun Syst 2011; 52: 2047-2058.

[7] Rutvji HJ, Patel SJ, Jinwala, DC. A novel approach for gray hole and black hole attacks in mobile ad hoc networks. In: IEEE 2012 Advanced Computing and Communication Technologies; 7–8 January 2012; Rohtak, Haryana, India: IEEE. pp. 556-560.

[8] Sakshi J, Ajay K. Detection techniques of black hole attack in mobile ad hoc network: A survey. In: ACM 2015 International Advanced Research in Computer Science Engineering and Technology Conference; 6–7 March 2015; New York, NY, USA: ACM.

[9] Anuj R, Rajeev P, Kapoor RK, Karaulia DS. Enhancement in security of AODV protocol against black hole attack in MANET. In: ACM 2014 International Information and Communication Technology for Competitive Strategies Conference; 14–16 November 2014; Udaipur, Rajasthan, India: ACM.

[10] Rajesh Y, Anil KS. Enhancing performance of AODV against black hole attack. In: ACM 2012 CUBE International Information Technology Conference; 3–6 September 2012; Pune, India: ACM. pp. 857-862.

[11] Venkanna U, Leela RV. Black hole attack and their counter measure based on trust management in MANET: A survey. In: IET 2011 Advances in Recent Technologies in Communication and Computing Conference; 14–15 November 2011; Bangalore, India: IEEE. pp. 232-236.

[12] Kanthe AM, Simunic D, Prasad R. Effects of malicious attacks in MANETs. In: IEEE 2012 Computational Intelligence and Computing Research Conference; 18–20 December 2012; Coimbatore, India: IEEE. pp. 1-5.

[13] Osathanunkul K, Ning Z. A countermeasure to black hole attacks in MANET, In: IEEE 2011 Networking, Sensing and Control Conference; 11–13 April 2011; Delft, Netherlands: IEEE. pp. 508-513.

[14] Inouye J, Binkley J, Walpole J. Dynamic network reconfiguration support for mobile computers. In: ACM 1997 Mobile Computing and Networking Conference; 26–30 September 1997; Budapest, Hungary: ACM. pp. 13-22.

[15] Gang W, Yong B, Jie L, Ogielski A. Interactions between TCP and RILP in wireless internet. In: IEEE 1999 Global Telecommunication Conference; 5–9 December 1999; Rio de Janeiro, Brazil: IEEE. pp. 661-666.

[16] Joseph JFC, Lee BS, Das A, Seet BC. Cross layer detection of sinking behavior in wireless ad hoc networks using SVM and FDA. IEEE T Depend Secure 2011; 8: 233-245.

[17] Usha G. Honeypot based single and cross layer black hole attack detection for MANET. PhD, Anna University, Chennai, India, 2014.