Asian Journal of Information Technology 15 (24): 4979-4985, 2016
ISSN: 1682-3915

Efficient DDoS Attack Detection Techniques for Privacy Protecting Routing Protocol in MANET

[1]E. Ahila Devi, [2]K. Chitra and [3]C. Selvakumar
[1]Anna University, Chennai, India
[2]School of Electronics Engineering, VIT University, Chennai, India
[3]St. Joseph's College of Engineering, Chennai, India

Abstract: In MANET, privacy protecting routing is a big challenge. To overcome this in this study we proposed to design efficient DDoS attack detection techniques for the PPSEER. We mainly consider Sybil and selective forwarding attacks. A legitimate node and a Sybil attack node are differentiated based on their neighborhood joining behavior using RSS. In the proposed solution, the super nodes (deployed in previous work) monitor their upstream and downstream nodes and estimate the RSS and link loss rate. While estimating the loss rate, both the losses in transmission due to bad channel quality and collision in the channel are considered. Each super node maintains a history of packet count for estimating link loss rate which is updated on receiving a packet from upstream node. Then a detection threshold was set up for RSS and link loss rate so as to detect the Sybil attacks and selective forwarding attacks.

Key words: Privacy protecting, estimating link, RSS, bad channel quality, neighborhood

INTRODUCTION

MANET: A MANET (Mobile Ad hoc Network) is a wireless ad-hoc network consists of a collection of two or more peer mobile nodes which can communicate with each other without any fixed infrastructure. Nodes within each other's radio range communicate directly via wireless links, whereas they utilize other nodes as relays or routers for those out of each other's radio range. In general, nodes share the same physical media and transmit and acquire signals at the same frequency band and follow the same hopping sequence or spreading code. MANET due to these features has several applications like emergency relief, military operations and terrorism response as these require no infrastructure (Shrestha *et al*., 2010; Bindra *et al*., 2012).

The intrinsic nature of lack of any centralized access control, secure boundaries (mobile nodes are free to join and leave and move inside the network) and limited resources in mobile ad-hoc networks make it vulnerable to several different types of passive and active attacks (Bindra *et al*., 2012; Chonka *et al*., 2008).

Efficient ddos attack detection for MANET: Distributed Denial of Service (DDoS) attack is one of the most alarming threats on the Internet. Nearly 4,000 DDoS attacks occur on the Internet every week. A DDoS attacker try to disrupt a target by flooding it with illegitimate requests for information, exhausting bandwidth and overtaxing servers so as to refuse its service to legitimate clients. The readily available software is used by the attacker uses to plant attack software on a large number of unprotected computers, generally known as zombies which become the launch pads for a DDoS attack at the attacke's command. The DDoS attacker usually disguises or spoofs the IP address section of a packet header so as to hide their identity from their victim. Hence create difficulty in tracking the attack source (Chen and Yonezawa, 2005; Chonka *et al*., 2008). DDOS attack can be classified into two as follows:

- Host attacks aim to starve a server of its resources by exploiting software flaws
- Bandwidth attacks attempt to disrupt a server by consuming all its network bandwidth (Chen and Yonezawa, 2005)

The legitimate nature of attacking hosts rise attack detection difficulty. Instead of sending illformatted network packets, attackers enable the zombies to comply with computer network regulations and request objects as they appear at pages, pretending to be legitimate users. Also, low rate arrival of zombies and their request frequency; make them look as system-friendly connections for rate-based Intrusion Detection Systems (IDS) (Chwalinski *et al*., 2013).

Corresponding Author: E. Ahila Devi, Anna University, Chennai, India

A Privacy Protecting Secure and Energy Efficient Routing Protocol (PPSEER) was proposed in our previous paper for providing a secure and energy efficient routing protocol. Wherein, the network nodes were classified according to their energy level. The node which has the sufficient energy level is called as super node which is used to forward the message. Then, encryption is performed based on group signature including additional secure parameter like secret key and maximum transmission power which is known only to the sender and recipient node. The advantage of the proposed routing protocol is that it increases privacy of the message as well as it maintains the energy efficiency of the node.

Literature review: Abbas *et al*. (2013) proposed a lightweight scheme for new identity Sybil attacker detection without any centralized trusted third party or any extra hardware, like directional antennae or a geographical positioning system. However, low transmission rates produce false positives especially when the speed is high.

Shila *et al*. (2010) developed a Channel Aware Detection (CAD) algorithm for effective identification of the selective forwarding misbehavior from the normal channel losses. The CAD algorithm depends on channel estimation and traffic monitoring. When the node's monitored loss rate at certain hops exceeds the estimated normal loss rate it will be identified as attackers. The optimal detection thresholds were determined to reduce the summation of false alarm and missed detection probabilities. However packet delivery ratio is on decreasing graph.

Xing and Wang (2010) proposed a novel semi-Markov process model for characterizing the evolution of node behaviors. Then, the network survivability was derived and the lower and upper bounds on the topological survivability for k-connected networks were derived. However goodput was decreased.

Nadeem and Howarth (2013) proposed a generalized intrusion detection and prevention mechanism using a combination of anomaly-based and knowledge based intrusion detection to secure MANETs from a wide variety of attacks so as to detect new unforeseen attacks.

Khalil and Bagchi (2011) presented SADEC protocol to detect and isolate stealthy packet dropping attack efficiently. It presented two techniques for local monitoring, i.e., having the neighbors maintain additional information about the routing path and adding some checking responsibility to each neighbor. In addition an innovative mechanism was provided for better utilize local monitoring by considerably increasing the number of nodes in a neighborhood which can monitor. However, the listening activity for detecting malicious behavior is more complicate. As an extension to this study we proposed to design efficient DDoS attack detection techniques for the PPSEER. We mainly consider Sybil and selective forwarding attacks.

MATERIALS AND METHODS

Overview: A legitimate node and a Sybil attack node are differentiated based on their neighborhood joining behavior using RSS (Abbas *et al*., 2013). In the proposed solution, the super nodes (deployed in previous work) monitor their upstream and downstream nodes and estimate the RSS and link loss rate. While estimating the loss rate, both the losses in transmission due to bad channel quality and collision in the channel are considered (Shila *et al*., 2010). Each super node maintains a history of packet count for estimating link loss rate which is updated on receiving a packet from upstream node. Then a detection threshold was set up for RSS and link loss rate so as to detect the Sybil attacks and selective forwarding attacks. There are notations used in this study:

- P_{LS}; Loss rate probability
- W_{CQ}; Wireless channel quality
- P_C; Packet collision probability
- T_p; The transmission power of sender
- TS; Time stamp
- TV; Threshold value
- R_P; Remaining power at wave at receiver
- G_T; Gain of transmitter
- GR; The gain of receiver

Sybil node detection: Based on neighborhood joining behavior, a new legitimate node and a new Sybil attack node are differentiated.

New legitimate node: As soon as a node enters inside the radio range of other that new legitimate nodes become neighbors and their fist RSS at the receiver node will be low enough.

Sybil attacker: it is cause because of already known neighbor. The already known neighboring node cause its new identity to appear abruptly in the neighborhood. the Sybil attacker creates new identity, the signal.

The main difference between a legitimate newcomer and Sybil identity is their entrance behavior. Each node

Node ID	RSS-list	Loss rate	Time stamp
1	R_1 T_1 R_2 T_2 R_n T_n	......	....
2		......	....
3		......	....
..		......	....
N		......	....

Fig. 1: Neighbor List Based on RSS and LR

maintains a list of neighbors in the form <NID, RSS<TS, RSS>> (Fig. 1) and records the RSS values of any directly received or overheard frames of 802.11 protocol, i.e., RTS, CTS, DATA and ACK messages.

Each node will capture and store the signal strength of the transmissions received from its neighboring nodes. This can be performed when a node either takes part in the communication directly with other nodes acting as a source or a destination or when a node does not take part in the direct communication.

In the latter case it will capture the signal strength values of other communicating parties through overhearing the control frames. Each RSS- List in front of the corresponding address contains R_n RSS values of recently received frames along with their time of reception, T_n. Where n is the number of elements in the RSS- List that can be increased or decreased depending upon the memory requirements of a node.

RSS and loss rate estimation: The super nodes (deployed in previous work) monitor their upstream and downstream nodes and estimate the RSS and link loss rate. Super nodes are selected for message forwarding services to other MANET nodes.

Each node in the network maintains a history of packet count to measure the link loss rate. When a node receives a packet from the upstream, it updates the packet count history with the corresponding packet sequence number. S is the source and D is the destination. The F_s denotes the number of packets forwarded by source S to destination D.

RSS estimation: The Received Signal Strength (RSS) offers a possibility to realize distance determination with minimal effort. RSS is a distance which measuring the received signal strength of the incoming radio signal. The RSS is that the configured transmission power at the transmitting device (T_P) directly affects the receiving power at the receiving device (R_P). Power of receiving device is calculated using the following Eq. 1:

$$R_P = T_P \times G_T \times G_R \left(\frac{\lambda}{4\prod d} \right)^2 \quad (1)$$

Where:

T_p = The transmission power of sender
R_P = The remaining power at wave at receiver
G_T = The gain of transmitter
G_R = The gain of receiver, e is the wave length
d = The distance between sender and receiver

In embedded devices, the received signal strength is converted to a Received Signal Strength Indicator (RSSI) which is defined as ratio of the received power to the reference power (P_{ref}). RSS value is calculated using the Eq. 2:

$$RSS = 10 \times \log \frac{R_P}{P_{ref}} \quad (2)$$

Loss rate estimation: While estimating the loss rate, both the losses in transmission due to bad channel quality and collision in the channel are considered. We estimate the loss due to wireless channel quality, by modeling the underlying time varying wireless channel as a two-state Markov Model (Gandikota *et al.*, 2008). The two-state Markov Model has two states, G and B which represents the good and bad states respectively. P_G is the losses occur in good states and the bad state they happen with a probability of P_B. If the transmission from A-G then probability of the model is defined as P_{AG}. The wireless channel quality (W_{CQ}) of the Markov channel is give:

$$W_{CQ} = P_G \times sp + P_B \times sp \quad (3)$$

In Eq. 3, sp is the steady state probability and can be computed. Since a wireless mesh network is normally deployed statically for long time, we assume that the channel parameters P_{AG}, P_{BG}, P_A and P_B can be accurately estimated by observing historical data.

In the MAC layer, a packet may be lost due to MAC layer collisions when multiple transmissions happen in the same slot. The packet collision probability for a given transmission, denoted as P_C, can be estimated by measuring the channel busyness ratio, denoted as C_{BR}.

The channel busyness ratio is defined as the proportion of time that the channel is in the status of successful transmission or collision. It is very convenient for a node to monitor the channel busyness ratio as a CSMA-based MAC protocol works on physical and virtual carrier sensing mechanisms. For a given observation window the channel idling time can be easily computed by tracing the backoff counter values, the leftover part within the observation window is the channel busy time.

Consider n is the total number of nodes competing the channel. Let P_t denote the probability that a node transmits in a certain time slot. For the MAC channel at steady state, the probabilities for observing an idle, successful and colliding slot (denoted as P_{idle}, P_{suces} and P_{coll}, respectively) can be expressed as:

$$\begin{aligned} P_{idle} &= (1-P_t)^n \\ P_{sucess} &= nP_t(1-P_t)^n \\ P_{coll} &= 1-P_{idle}-P_{sucess} \end{aligned} \quad (4)$$

The channel busyness ratio can then be computed as:

$$C_{BR} = 1 - p \quad (5)$$

$$p = \frac{P_{idle}\times t}{P_{idle}\times t+P_{sucess}\times t+P_{coll}\times t} \quad (6)$$

In Eq. 6 where t is the idle slot length, the duration of a successful transmission and the duration of a collision, respectively which can be determined from the 802.11 standard The packet collision probability P_c is the probability that one node encounters collisions when it transmits which is linked to the probability P_t as:

$$P_c = 1-(1-P_t)^{n-1} \quad (7)$$

Considering both the effects of bad channel quality and medium access collisions, the aggregate normal loss rate can be expressed as follows:

$$P_{LS} = W_{CQ}+P_c \quad (8)$$

To improve the successful delivery rate of a packet, packet loss rate is required.

Ttack detection technique: Consider the new node zone A and B. when new nodes enter into the node A, it will calculate the RSS value of that new node. Based on the calculated RSS value, node A can easily differentiate between a new node B that is coming into its neighborhood and an identity created by a Sybil attacker, pretending to be a new node joining the neighborhood.

Algorithm 1: Attack detection technique

```
Start
Define TV = Threshold value
LS = Loss rate
RSS = Received Signal Strength
TS = Time Stamp
When new node enter into the new zone
{
If (RSS and LR > threshold)
Node in white zone
Else if (RSS and LR < TV)
Node in gray zone
}
For (every TS)
{
RSS and LR values are updated in RL table
New RSS and LR values are compare with the updated table values with
their node ID and TS
If (RSS a& LR > NEW_TV)
 {
Add that node ID into malicious node list
Sent that node ID to the other node as a malicious node
}
End
```

Node A will make a decision based on the RSS value and loss rate. If the first RSS value captured is greater than the threshold, i.e., a node is in the white zone A will deem that identity as a new identity from a Sybil attacker, since no node can penetrate into white zone within the specified speed. If the first RSS value received is less than the threshold, i.e., a node is in the gray zone, it will be considered as a normal new entrant and will be added to the neighbor list. Upon detection of Sybil identity, the detector node will inform its 1-hop neighbors by transmitting a special detection update packet. Each node when receives two or more than two packets from two distinct nodes about an identity to be Sybil that identity will be deemed as Sybil identity (Fig. 2).

RSS values are updates for each time stamp and if the address is not in the RSS table, meaning that this node has not been interacted with before, i.e., it is a new node and the RSS received is its first acknowledged presence. This first received RSS is compared against an new-threshold (this threshold is used to check using the RSS whether the transmitter is in white zone). If it is greater than or equal to the threshold indicating that the new node lies near in the neighborhood and did not enter normally into the neighborhood the address is added to the malicious node list. Otherwise, the address is added to the RSS table and a link list is created for that address in order to store the recently received RSS along with its time of reception in it. Finally, the size of the link list is checked if it is greater than the list-ize, the oldest RSS is removed from the list. Table 1, RSS and LR values are stored. To control the table size, the unused records need to be deleted.

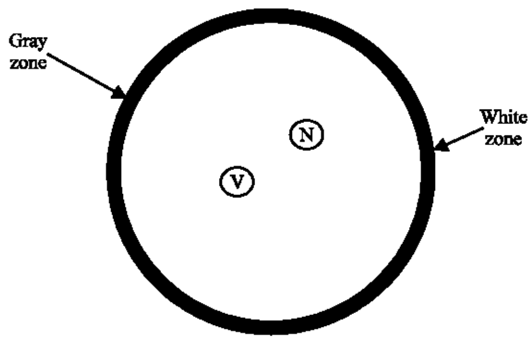

Fig. 2: Node zone A

Table 1: RSS and LR values

Parameters	Values
No. of nodes	20 and 100
Area size	500×500
Mac	IEEE 802.11
Transmission range	250 m
Simulation time	50 sec
Traffic source	CBR
Packet size	512
Sources	4
Rate	50 kb
Attackers	2
Initial energy	7.1J
Transmission power	0.375
Receiving power	0.375
Flows	2, 4, 6 and 8

These unused records are due to certain reasons. First when a malicious node changes its identity, its previous identity record stays in the RSS table.

For each time stamp the values are updated with their node ID. The node zone will compare the existed node records to check whether it is malicious node or not. If the same node sends the two RSS and LR values then it is said to be malicious node. When the node marked as malicious node that node is deleted from the node list.

RESULTS AND DISCUSSION

Smulation model and parameters: The Network Simulator (NS2) is used to simulate the proposed architecture. In the simulation, the mobile nodes move in a 500×00 m region for 50 sec of simulation time. All nodes have the same transmission range of 250 m. The simulated traffic is Constant Bit Rate (CBR). he simulation settings and parameters are summarized in table.

Performance metrics:h proposed Efficient DDoS Attack Detection techniques for Privacy Protecting Routing Protocol (EDADPPR) is compared with the LSA technique

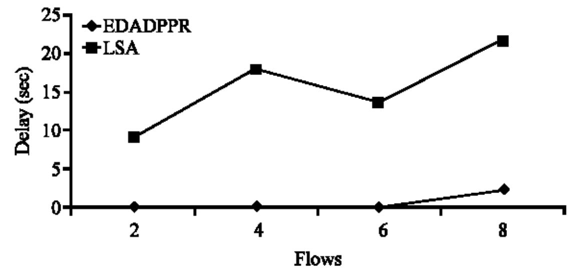

Fig. 3: Flows vs. delay

The performance is evaluated mainly, according to the following metrics.

Packet delivery ratio: It is the ratio between the number of packets received and the number of packets sent.

Packet drop: It refers the average number of packets dropped during the transmission.

Energy consumption: It is the amount of energy consumed by the nodes to transmit the data packets to the receiver.

Delay: It is the amount of time taken by the nodes to transmit the data packets.

Case-1 (For-20 nodes scenario)

Based on flows: In our experiment we vary the number of flows as 2, 4, 6 and 8.

Figure 3 shows the delay of EDADPPR and LSA techniques for different number of flows scenario. We can conclude that the delay of our proposed EDADPPR approach has 97% of less than LSA approach.

Figure 4 shows the delivery ratio of EDADPPR and LSA techniques for different number of flows scenario. We can conclude that the delivery ratio of our proposed EDADPPR approach has 58% of higher than LSA approach

Figure 5 shows the drop of EDADPPR and LSA techniques for different number of flows scenario. We can conclude that the drop of our proposed EDADPPR approach has 95% of less than LSA approach.

Figure 6 shows the energy consumption of EDADPPR and LSA techniques for different number of flows scenario. We can conclude that the energy consumption of our proposed EDADPPR approach has 4% of less than LSA approach.

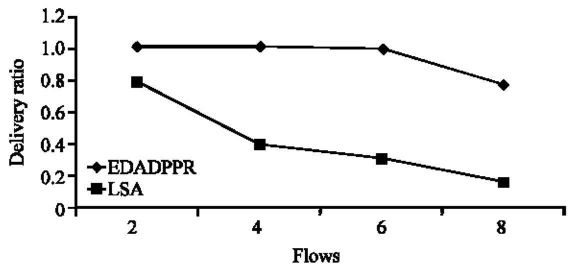

Fig. 4: Flows vs. delivery ratio

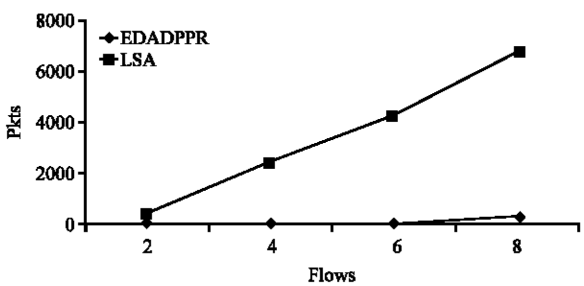

Fig. 5: Flows vs. drop

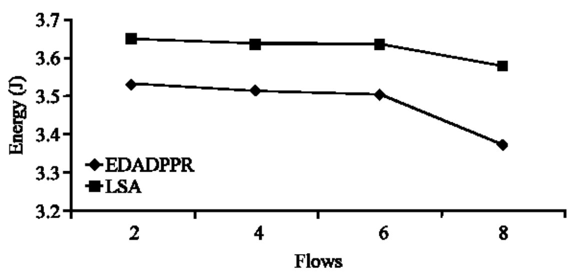

Fig. 6: Flows vs. energy consumption

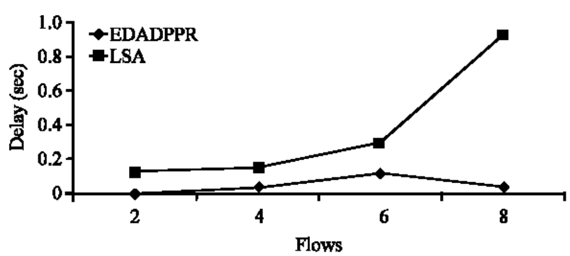

Fig. 7: Flows vs. delay

Case-2(For-100 nodes scenario)

Based on flows: In our experiment we vary the number of flows as 2, 4, 6 and 8. Figure 7 shows the delay of EDADPPR and LSA techniques for different number of flows scenario. We can conclude that the delay of our proposed EDADPPR approach has 80% of less than LSA approach.

Figure 8 shows the delivery ratio of EDADPPR and LSA techniques for different number of flows scenario. We can conclude that the delivery ratio of our proposed EDADPPR approach has 27% of higher than LSA approach.

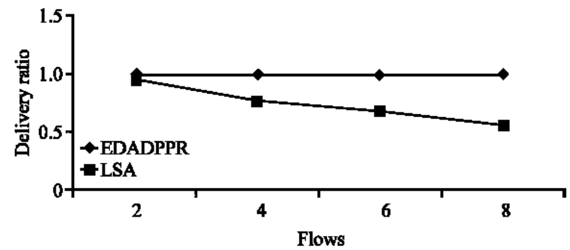

Fig. 8: Flows vs. delivery ratio

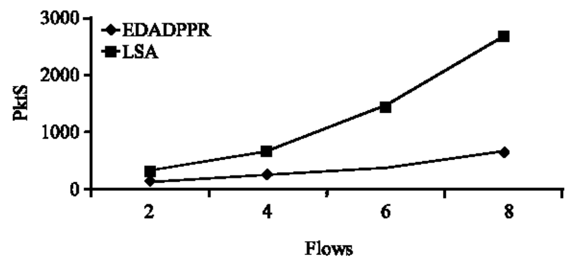

Fig. 9: Flows vs. drop

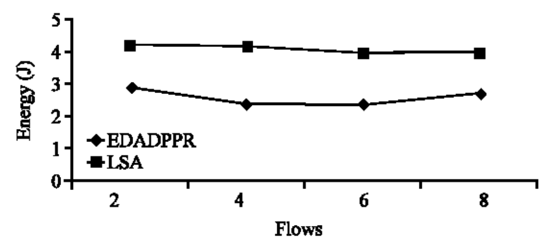

Fig. 10: Flows vs. energy consumption

Figure 9 shows the drop of EDADPPR and LSA techniques for different number of flows scenario. We can conclude that the drop of our proposed EDADPPR approach has 67% of less than LSA approach.

Figure 10 shows the energy consumption of EDADPPR and LSA techniques for different number of flows scenario. We can conclude that the energy consumption of our proposed EDADPPR approach has 37% of less than LSA approach.

CONCLUSION

As an extension to previous research in this study we proposed to design efficient DDoS attack detection techniques for the PPSEER. A legitimate node and a Sybil attack node are differentiated based on their neighborhood joining behavior using RSS. In the proposed solution, the super nodes (deployed in previous work) monitor their upstream and downstream nodes and estimate the RSS and link loss rate. While estimating the loss rate, both the losses in transmission due to bad channel quality and collision in the channel are considered. Each super node maintains a history of packet count for estimating link loss rate which is updated on receiving a packet from upstream node. Then a detection threshold was set up for RSS and link loss rate so as to detect the Sybil attacks and selective forwarding attacks. We mainly consider Sybil and selective forwarding attacks.

REFERENCES

Abbas, S., M. Merabti, J.D. Llewellyn and K. Kifayat, 2013. Lightweight sybil attack detection in MANETs. IEEE. Syst. J., 7: 236-248.

Bindra, G.S., A. Kapoor, A. Narang and A. Agrawal, 2012. Detection and removal of co-operative blackhole and grayhole attacks in MANETs. Proceedings of the 2012 International Conference on System Engineering and Technology (ICSET), September 11-12, 2012, IEEE, Haryana, India, ISBN: 978-1-4673-2375-8, pp: 1-5.

Chen, E.Y. and A. Yonezawa, 2005. Practical techniques for defending against DDoS attacks. Proceedings of the 3rd ACS/IEEE International Conference on Computer Systems and Applications, January 6-6, 2005, IEEE, Tokyo, Japan, ISBN: 0-7803-8735-X, pp: 72-72.

Chonka, A., W. Zhou, J. Singh and Y. Xiang, 2008. Detecting and tracing DDoS attacks by intelligent decision prototype. Proceedings of the Sixth Annual IEEE International Conference on Pervasive Computing and Communications PerCom 2008, March 17-21, 2008, IEEE, Geelong, Victoria, Australia, ISBN: 978-0-7695-3113-7, pp: 578-583.

Chwalinski, P., R. Belavkin and X. Cheng, 2013. Detection of application layer DDoS Attacks with clustering and bayes factors. Proceedings of the 2013 IEEE International Conference on Systems, Man and Cybernetics, October 13-16, 2013, IEEE, London, UK., ISBN: 978-1-4799-0652-9, pp: 156-161.

Gandikota, V.R., B.R. Tamma and C.S.R. Murthy, 2008. Adaptive FEC-based packet loss resilience scheme for supporting voice communication over ad hoc wireless networks. IEEE. Trans. Mob. Comput., 7: 1184-1199.

Khalil, I. and S. Bagchi, 2011. Stealthy attacks in wireless ad hoc networks: Detection and countermeasure. IEEE Trans. Mobile Comput., 10: 1096-1112.

Nadeem, A. and M. Howarth, 2013. Protection of MANETs from a range of attacks using an intrusion detection and prevention system. Telecommun. Syst., 52: 2047-2058.

Shila, D.M., Y. Cheng and T. Anjali, 2010. Mitigating selective forwarding attacks with a channel-aware approach in WMNs. IEEE. Trans. Wirel. Commun., 9: 1661-1675.

Shrestha, R., K.H. Han, D.Y. Choi and S.J. Han, 2010. A novel cross layer intrusion detection system in MANET. Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications, April 20-23, 2010, Perth, WA., pp: 647-654.

Xing, F. and W. Wang, 2010. On the survivability of wireless ad hoc networks with node misbehaviors and failures. IEEE. Trans. Dependable Secure Comput., 7: 284-299.