ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(38), DOI: 10.17485/ijst/2016/v9i38/99301, October 2016* ISSN (Online) : 0974-5645

COBAST: Node Eminence State and Cooperative Bait Strategy based Route Discovery to Prevent Black and Gray Hole Attacks in Mobile Ad hoc Networks

G. Soma Sekhar[1*] and E. Sreenivas Reddy[2]

[1]Department of CSE, Acharya Nagarjuna University, Guntur - 522510, Andhra Pradesh, India; somasekharonline@yahoo.co.in

[2]College of Engineering, Acharya Nagarjuna University, Guntur - 522510, Andhra Pradesh, India; esreddy67@gmail.com

Abstract

Objectives: The data transmission in Mobile ad hoc networks (MANETs) usually compromises to security issues due to their dynamic topology. One of the malicious acts of the compromised nodes is Black hole attack, which becomes a significant research challenge. **Methods/Analysis**: We proposed a Node Eminence State and Cooperative Bait Strategy (COBAST) based Secure Route discovery to prevent the selection of route with nodes prone to black hole attack. This contribution is an extension of our earlier model ENES. The cooperative bait strategy proposed here is discovering the suspicious nodes involvement in the selected route. The experiments were done using NS2 simulator and simulated the network with presence of divergent ratios of malicious nodes. The performance of the proposal is estimated by comparing with the results obtained from other model found in contemporary literature, which is labeled as CBDA. **Findings:** The conventional metrics such as end to end delivery ratio, delay and routing overhead were assessed and also performed the experiments to assess the accuracy sensitivity and specificity of black hole node discovery. The obtained results for the metrics adapted were confirming the scalability and robustness of the COBAST. **Novelty/Improvement**: The proposed model evinced the scalability and robustness in detection of black hole attack prone nodes under minimal computational cost. The route discovered under the proposed model also found to be optimal in end to end maximum packet delivery ratio, minimum delay.

Keywords: Black Hole Attacks, COBAST, Cooperative Bait Strategy, Mobile Ad Hoc Network (MANET), Node Eminence Score

1. Introduction

The role of wireless mobile devices is phenomenal to fulfill the communication needs in real time scenarios such as military operations, handling nature disasters. The mobile ad hoc network is a pool of mobile nodes that uses no physical medium to communicate. Each node capable to communicate with other nodes exists in a specific range of their radio frequency. Hence the node that intended to transmit data to other node which is not in its transmission range, establishes a route between them using the connected hop level nodes (nodes in transmission frequency range). Since the communication between nodes depends on radio links and the network topology is dynamic, the established routes are vulnerable to divergent security threats, which causes data loss due to link failures, selfish nodes, black holes and other malevolent activities of malicious nodes[1-4]. Henceforth, establishing a secure route with minimal process overhead is a significant requirement for mobile ad hoc networks[4]. The proactive, reactive and hybrid are the default categories of the routing protocols[5,6] in mobile

* *Author for correspondence*

ad hoc networks. Under proactive strategy, the nodes exchange the information related to routing topology at specific intervals, which leads to process overhead. In contrast to this, under reactive strategy, the route will be established on demand.

In regard to the security of dynamic routing, defending the black hole attack is challenging[4].The scenario of this attack is that a compromised node initiates a forged route response such that it contains a shortest path to destination. Once the route established through that compromised node, then it drains the transmitted packets without sending to the destination. Hence the many of research contributions in contemporary literature proposed novel route discovery strategies with aim defending black hole attacks.

Recently, many proposals had been proposed in defending, avoiding and detecting black hole nodes in mobile ad hoc networks[7,8].

The proactive strategy of malicious node defending approaches[9-15] enables to notify the compromised behavior of the nearby nodes. The significant constraint of these models is process overhead due to the act of collecting the topological status of the nearby nodes in periodical intervals. This periodical neighbor state update process considerably costs performance of routing and evinces resource utilization overhead and process overhead, particularly if network with the absence of malicious nodes. But this proactive strategies helps to prevent role of malicious nodes in routing at initial stage. In contrast to the proactive strategies, the reactive defense mechanisms[16-18] initiates to detect the malicious node involvement in routing if considerable packet loss noticed by destination node. The constraint of the reactive defense mechanisms is that initiates detection of malicious nodes after a significant packet loss.

A proactive strategy[12] was proposed to detect the malicious node involvement in selected route. The successful transmission of packets at two hop level will be acknowledged in converse direction of the route. This scheme evinces routing overhead, which is a general constraint of the proactive defense mechanisms.

A reactive defense mechanism[16] called Best-effort Fault-Tolerant Routing (BFTR). This strategy relies on the acknowledgements sent by the destination node to source about the state of routing path. The acknowledgement received by the source from the destination contains the end to end packet delivery ratio and delay. According to the dropouts found in packet delivery ratio and escalation observed in delay, the source node triggers to alternative route to avoid the packet drops. The BFTR scheme is failed to confirm that the alternative route is not included the malicious nodes, hence the route discovery process can be recursive, which leads to substantial process overhead.

Localized Secure Routing Architecture[19] was proposed that aimed to defend cooperative black hole attacks. The model is reactive strategy that depends on a security monitoring node to estimate the abnormal delay occurred due to black hole attack prone nodes involved in route. This strategy is evinced fine-tuned detection scope but limited to the level of route maintenance, also the optimal route discovery is not addressing the discovery of malicious nodes involvement in selected route. Further the experimental results evinced the process overhead.

Another contemporary contribution observed in recent literature is DNA-Based Cryptographic Mechanism[20]. This is also a reactive strategy with considerable process overhead, which is due to the involvement of cryptographic standards used.

A Cooperative Bait Detection Approach (CBDA)[21] was proposed, which is similar strategy of our contribution to defend the Collaborative Attacks by Malicious Nodes. This also found to be a reactive strategy that discovers and defends malicious nodes during the routing process. The experimental study evincing the process overhead against significant ratio of malicious nodes involvement. This model also not addressing the detection of malicious node involvement at route discovery.

In order to this, our contribution aimed to define a secure route discovery strategy that estimates the optimality of the route based on the eminence scope of the intermediate nodes and malicious attack proneness. The proposed mechanism is node eminence state and cooperative bait strategy (COBAST) based secure route discovery to prevent black hole attack in mobile ad hoc networks, which reflects the characteristics of proactive defense mechanisms with one time discovery of node's topological state. Henceforth the default constraint called process overhead of proactive defense mechanisms is not evinced in the proposed scheme. Unlike the secure route discovery model CBDA that selects nearest hop node as bait node (which may be compromised often), the COBAST selects a hop level node with maximal eminence score as bait node. In order to this, node eminence scope is estimated by using our earlier contribution ENES[22]

and further uses cooperative bait strategy, which is the main contribution of this manuscript to identify the involvement of the malicious nodes during optimal route discovery. The topological state of the nodes involved in the route will verified at optimal route selection by COBAST, if found to be the selected route is malevolent then only it considers next optimal route and initiates the Bait strategy to discover the role of malicious nodes in the selected route. This practice (if current route found to be malevolent then only considers the next optimal route) reflects the property of reactive defense strategies.

The rest of the paper explores the proposed model in section 2 that followed by section 3, which is describing the experimental study. The section 4 concludes the contributions of the manuscript.

2. Node Eminence State and Cooperative Bait Strategy based Route Discovery

Estimating and updating the eminence scope of a node involved in ad hoc routing was explored in our earlier contribution called ENES[22]. The metrics used in ENES are limited to identify the selfish nodes and nodes with under rated QoS factors. In order to discover the nodes with malicious act, in particular black hole attack prone, the ENES is extended to perform cooperative bait strategy to discover secure routes to avoid black hole attacks. In a gist, the cooperative bait strategy initiates to discover possible routes between each node n involved in the selected route r and a hop level node as bait node bn with maximal eminence score respective to that $node_n$. If any of the node that involved in discovered routes that is not a hop level node to either the node n or node bn is labeled as suspicious node. Then the route is confirmed as prone to malicious act if any of the discovered suspicious nodes found the respective route r The process flow of the proposed model is as follows:

- **Route Selection**

1. Perform route selection by conditional broadcasting strategy
2. Order the selected routes in descending by their routing optimality rank(aggregate eminence score of the route can be used to estimate the route optimality)

- **Malicious node detection (see sec 2.2**

1. Choose the optimal route from the response routes found in route selection
2. For each node in the source route as source
   a. select hop level node (as bait) with high eminence score (see sec 2.1) as target and perform route request
   b. For each route found from the route response
      i. for each intermediate node of the route
      - if intermediate node is the ho level node for source and bait node then consider that node as fair enough then notify that node as -ve to malicious act
      - else notify the node as positive to malicious act

      End //of i
   End // of b
End //end of 2
3. Found the similarity between the set of nodes involved in optimal route selected and the set of nodes labeled as positive to malicious act by jaccard similarity index
4. if similarity found to be greater than 0, then discard the optimal route selected and repeat the steps 1 to 4
5. confirm the optimal route selected as route to transmit the data
6. Perform the act of eminence update for all nodes involved in the selected route (see sec 2.3)

2.1 Route Discovery

The initial step to discover the secure route by the proposed model is to locate all possible routes to transmit data between selected source and destination node by using the qualified diffusion of the route request[18]. Let $R = \{r_1, r_2, ...r_{|R|}\}$ be the set of routes selected in route request process[18].

2.2 Assessing the Current Eminence Score

The eminence score of a node is estimated by our earlier contribution ENES[22]. Briefing of the metrics used and eminence score calculation follows.

- Aptitude Deflection (iad) : The diffused capacity of transmission load is (no diffusion (+1), diffusion caused by shared resource (0), or diffusion caused by malicious activity (-1)).
- Consistency Deflection (icd) : The diffusion of ingress and egress ratio (no diffusion (+1), diffusion caused by shared resource (0), or diffusion caused by malicious activity (-1)).
- Rectitude Deflection (ird) : The performance diffusion without external impacts (no diffusion (+1),

diffusion caused by shared resource (0), or diffusion caused by malicious activity (-1)).

The three states of these three metrics are no diffusion, diffusion due to shared resource and diffusion due to malicious act, which are ranked +1, 0 and -1 respectively.

Then assessing eminence score of the node is as follows:

$$es = \begin{cases} \dfrac{iad + icd + ird}{\sqrt{(iad + icd + ird)^2}} & if\ (iad + icd + ird) \neq 0 \\ 0 & if\ (iad + icd + ird) \equiv 0 \end{cases} \quad (1)$$

2.3 Malicious Node Detection by Cooperative Bait Strategy

The suspected nodes in the context of each node n involved in the selected optimal route $\{r \exists r \in R\}$ will be identified initially. In order to identify the suspicious nodes, each node $\{n \exists n \in r\}$ as source node, selects a hop node with maximal eminence score as bait node bn and then initiates route request to the node bn Upon completion of the route response, collects all possible routes between node n and node bn. Further assess the state of each intermediate node itn involved in each discovered route tr is suspicious to malicious act or not. The intermediate node that is hop level node to neither node n nor node bn is labeled as suspicious and registers that node in to the suspicious node list snl Upon completion of the suspicious node discovery process by each node involved in route r, the route r is prone to black hole or not is estimated as follows. The route r is said to be attack prone if $|\{snl \bigcap r\}| \neq 0$ (the set of the nodes observed in both route and suspicious nodes list is empty) else the route r is recommended to routing process. If selected optimal route found to be suspicious then the cooperative bait strategy is applied on the next optimal route $\{r \exists r \in R\}$. This process continues till the discovery of a secure route from the route list R The metrics used here in this proposed model to identify a route is attack prone or not under cooperative bait strategy are (1) suspicious nodes at hop level and (2) suspicious nodes at route level. The significance of adapting these metrics are:

3. Hop level Suspicious nodes: The nodes that are not the hop level nodes to either of the source node and bait node are found be suspicious since the routes discovered between a node and its hop level node are strictly formed with the nodes those are hop level nodes to either source or destination nodes.

4. Route Level Suspicious Nodes: A node that is hop level node to either of the source and destination nodes can also be attack prone. Hence the suspicious node discovery is done for all nodes involved in the optimal routes

The algorithmic exploration of the Cooperative Bait Strategy is as follows:

Let $snl \leftarrow \phi$ // an empty suspicious nodes list

1. $\overset{|R|}{\underset{i=1}{\forall}}\{r_i \exists r_i \in R\}$ Begin

a. $\overset{|r_i|}{\underset{j=1}{\forall}}\{n_j \exists n_j \in r_i\}$ begin

b. $en_{n_j} \leftarrow selectEHN(n_j)$ // selecting hop level node with maximal eminence respective to node n_j (see sec 3.2)

c.. $brl \leftarrow dbrl\left(n_j, e_{n_j}\right)$ find all routes between node n_j and node e_{n_j} (see sec 3.1)

d. $\overset{|brl|}{\underset{k=1}{\forall}}\{br_k \exists br_k \in brl\}$ begin // for each route in brl

e. $\overset{|br|}{\underset{l=1}{\forall}}\{n_l \exists n_l \in br\}$ begin //for each node in br

$if\left(n_l \notin \left\{hl_{n_j}\right\} \wedge n_l \in \left\{hl_{e_{n_j}}\right\}\right)$

// if node n_l is not in the list of hop level nodes $\left\{hl_{n_j}\right\}$ of node n_j and not in the list of hop level nodes $\left\{hl_{e_{n_j}}\right\}$ of node e_{n_j}

g $snl \leftarrow n_l$ //add node to suspicious nodes list snl

h.End // end of f

i.End //end of e

j.End // end of d

k.End //end of a

l. $cn \leftarrow \{r_i\} \bigcap \{snl\}$ // list of common nodes cn in route r_i and suspicious nodes list snl

m. $if\left(|cn| \equiv 0\right)$ begin // if common nodes list is empty

n.Claim the r_i is secure and optimal route

o.Exit //exit the loop in 1

p.End // end of m

2. End // end of 1

2.4. Eminence Score Update

Upon completion of the routing process, then each node n revises the eminence score factors of its successive node h_i found in the route as $es(h_i) + es_r(h_i)$. Here $es(h_i)$ is actual eminence score of the successive node h_i, $es_r(h_i)$ is eminence score of h_i observed during the

data transmission over the route r. Further the eminence score update is done as follows:

The each node n involved in route r prepares update message esu and sends to successive node h in current route rt_i, In regard to this, the node n relies on camouflage publishing approach (Unless accept and publish, message cannot be viewed). The encrypted format $ees(h)$ of the new eminence score $es(h)$ that XOR with a salt s. Further the signature $sig(h)$ of the node h that reflects the new eminence score will be created. Further the message esu that contains $ees(n_i)$ and $sig(h)$ will be sent to node h.

To restrict the scope of conditional acceptance of the new eminence score by the node h, the salt s used to XOR the $es(h)$ will sent to successive node h if and only if the new signature received by the node h should be published to its neighbor nodes. Further node h decrypts $ees(h)$ and then performs XOR operation on $es'(h)$ and s that results actual $es(h)$. Afterwards node h updates its eminence score factors.

Upon completion of the updating the eminence score of the node n_i, source node publishes $sig(n_i)$ to all other nodes through message broadcasting strategy.

3. Experimental Study

The performance of the COBAST is explored under multiple dimensions. In one dimension, traditional route performance assessment metrics such as end to end "ratio of packet delivery" and "delay" were analyzed, on other dimension, the malicious node detection accuracy and sensitivity was assessed and also determined the process complexity. In order to estimate the accuracy and sensitivity at malevolent nodes discovery, the cached routes prior knowledge of malicious nodes involvement were used as input for bait strategy proposed (see sec 2.2). The results obtained for metrics considered were compared with other model called CBDA[21], which is also a cooperative bait based malicious node detection strategy.

A computer with i5 processor, 4GB ram were used for experimental study. In order to assess the routing performance, the simulation of the mobile ad hoc network under desired topology was done usingNS2. The specifications used to simulate the network were explored in Table 1.The malevolent node detection accuracy and sensitivity analysis of proposed bait strategy was done using explorative language R[23,24].

The end to end delay observed for CBDA is not stable (see Figure 1) which is found very low under the impact of malicious nodes involved at the ratio of 0.08. But delay the delay evinced by CBDA at the increased ratio of malicious nodes (0.12, 0.16 and 0.2) is high that compared to the delay observed for COBAST. The COBAST delivers the linearity to restrict end-to-end delay under divergent ratio of malicious nodes (see Figure 1).

The Figure 2 evincing the downgraded performance of the CBDA to maintain the optimal packet delivery ratio under divergent ratio of malicious nodes that compared to COBAST. The COBAST is evincing the magnitude and stable performance in packet delivery ratio, since the optimal avoidance of the malicious nodes in route discovery by proposed bait strategy (see Figure 2).

The routes formed from 28 malicious nodes and 145 normal nodes were used for statistical assessment of the accuracy and sensitivity to discover the malevolent and normal nodes. Further the nodes labeled by COBAST and CBDA as malicious and normal from the given input routes were classified as true-positives (nodes identified as malevolent, which are actually malevolent), false-positives (nodes notified as malevolent, which are actually normal), true-negatives (nodes notified as normal, which are actually normal) and false-negatives (nodes notified as normal, which are actually malevolent). Further the statistical metrics (Powers, 2006) called precision, sensitivity, specificity and accuracy (see Table 2) were assessed for both COBAST and CBDA. The results evinced that the COBAST is more sensitive (93%) to detect malicious nodes that compared to the sensitivity observed for CBDA (76%).The overall detection accuracy of COBAST is 97% which is 9% more than the accuracy observed for CBDA (88%). The process complexity observed for the COBAST is linear (see the Figure3), hence the model (COBAST) proposed is scalable and robust.

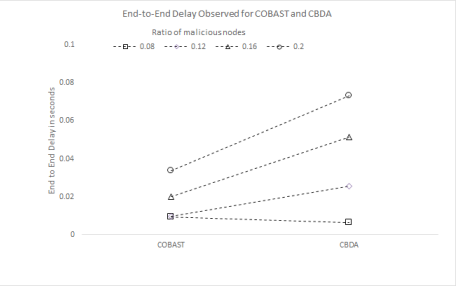

Figure 1. The end to end delay observed for COBAST and CBDA.

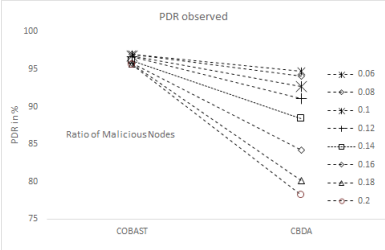

Figure 2. The Packet Delivery Ratio observed for COBAST and CBDA.

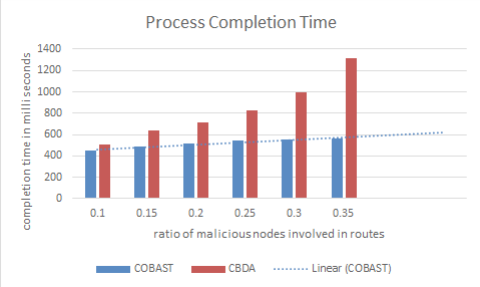

Figure 3. Completion time observed for divergent ratio of malicious nodes involvement in input routes.

Table 1. The list of simulation parameters

Frequency range of the Nodes	5 to 25 meters
Node velocity	Between 1m and 2.0m/sec
MAC specification	MAC 802.11 DCF
Network coverage	1500 X 2200 m2
Transmission Load in MB per Second	Between 1.0 and 2.5
Bandwidth in MB per Second	2.5
Transmission Type	CBR
Execution time	900 Sec

Table 2. Prediction ratios and assessment metric values observed

The metrics	Values observed for COBAST	Values observed for CBDA
Total Number of routes with malicious nodes involvements	32	32
Malicious Nodes Count	28	28
Normal of Fair Nodes Count	145	145
Total Number of nodes traced as malicious	30	35
Total number of nodes traced as normal	143	138
True Positives (truly predicted as malicious node)	26	21
False Positives (falsely predicted as malicious node)	4	14
True Negatives (Nodes truly predicted as normal)	141	131
False Negative (Nodes falsely predicted as normal)	2	7
Precision	0.866666667	0.6
Sensitivity	0.928571429	0.75
Specificity	0.972413793	0.903448276
Accuracy	0.965317919	0.878612717

4. Conclusion

We report a novel mechanism to defend the role of black hole nodes in secure route discovery for mobile ad hoc network. The proposed model is labeled as Node Eminence State and Cooperative Bait Strategy based secure route discovery to prevent black hole attack in Mobile ad hoc networks, which is reflecting the properties of proactive and reactive defense mechanisms. Unlike the traditional proactive defense mechanisms that observes the topological state of the neighbor nodes in periodical intervals, the proposed model is estimating the topological state of the nodes involved in the response routes only once during the optimal route selection. Hence the common constraint called process overhead of the proactive mechanisms is not evinced in the proposed model. If a route found with the involvement of black hole nodes, then only it applies bait strategy to discover the black hole nodes involvement in alternative route, which is similar to the property of reactive defense mechanisms. The experimental study evincing the scalability and robustness of the proposed model that compared to the similar strategy called CBDA found in recent literature. The future direction of the research can extend this model further to defend other malicious acts such as grey hole and vampire attacks.

5. References

1. Zhou L, Haas Z. Securing ad hoc networks. IEEE Network Magazine. 1999; 13(6):24–30.
2. Zapata M, Asokan N. Securing ad hoc routing protocols. In Proceedings of 3rd ACM workshop WiSE, USA. 2002; 1–10.
3. Papadimitratos P, Haas H. Secure data transmission in mobile ad hoc networks. In Proceedings of ACM workshop WiSE. 2003; 1(1):41–50.

4. Jabamani SS, Rajinikanth E. Integrity Key based Mechanism to Debase Packet Dropping in Manets. Indian Journal of Science and Technology. 2016; 9(14):1–4.
5. Sanzgiri K, Dahill B, Levine BN, Shields C, Belding-Royer EM. A secure routing protocol for ad hoc network. In Proceedings of 10th IEEE International Conference in Network Protocols (INCP' 02) IEEE Press, USA. 2002. p. 78–87.
6. Deng H, Agarwal P. Routing security in wireless ad hoc networks. IEEE Communication Magazine. 2002; 40(10):70–5.
7. Chang JM, Tsou PC, Chao HC, Chen JL. CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture. 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE), IEEE, Taiwan. 2011. p. 1–5.
8. Corson S, Macker J. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, RFC 2501. 1999.
9. Baadache A, Belmehdi A. Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks. 2010; 7(1):1–7.
10. Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking ACM, USA. 2000. p. 255–65.
11. Vishnu K, Paul AJ. Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks. International Journal of Computer Applications. 2010; 1(22):38–42.
12. Liu K, Deng J, Varshney PK, Balakrishnan K. An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Transactions on Mobile Computing. 2007; 6(5):536–50.
13. Deng H, Li W, Agrawal DP. Routing security in wireless ad hoc networks. IEEE Communications Magazine. 2002; 40(10):70–5.
14. Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard KE. Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. In International Conference on Wireless Networks. 2003. p. 570–5.
15. Weerasinghe H, Fu H. Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. In Future Generation Communication and Networking (fgcnIEEE. Oakland. 2007; 2:362–7.
16. Xue Y, Nahrstedt K. Providing fault-tolerant ad hoc routing service in adversarial environments. Wireless Personal Communications. 2004; 29(3-4):367–88.
17. Kozma W, Lazos L. REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits. In Proceedings of the Second ACM Conference on Wireless Network Security, ACM, USA. 2009. p. 103–10.
18. Wang W, Bhargava B, Linderman M. Defending against collaborative packet drop attacks on MANETs. In 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS (in Conjunction with IEEE SRDS New York, USA. 2009; 27:1–6.
19. Poongodi T, Karthikeyan M. Localized Secure Routing Architecture Against Cooperative Black Hole Attack in Mobile Ad Hoc Networks. Wireless Personal Communications. 2016; 1–12.
20. Babu ES, Nagaraju C, Prasad MK. Efficient DNA-Based Cryptographic Mechanism to Defend and Detect Black hole Attack in MANETs. In Proceedings of International Conference on ICT for Sustainable Development Springer Singapore. 2016. p. 695–706.
21. Chang JM, Tsou PC, Woungang I, Chao HC, Lai CF. Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. IEEE Systems Journal. 2015; 9(1):65–75.
22. Sekhar S, Reddy ES. ENES: Exploratory Node Eminence State for Secure Routing in Mobile Ad hoc Networks. International Journal of Applied Engineering Research. 2016; 11(8):5863–8.
23. Ihaka R, Gentleman R. R: a language for data analysis and graphics. Journal of Computational and Graphical Statistics. 2001; 5(3):299–314.
24. Amiri R, Rafsanjani M K, Khosravi E. Black hole attacks detection by invalid ip addresses in mobile ad hoc networks. Indian Journal of Science and Technology. 2014; 7(4):1–8.