NESSRD: Node Eminence State and Node Sequence State based Secure Route Discovery to Prevent Black and Gray Hole Attacks in Mobile Ad Hoc Networks

G. Soma Sekhar* and Dr. E. Sreenivas Reddy **
*Research Scholar, Department of CSE, Acharya Nagarjuna University, AP, India
Email: gsomasekharonline@gmail.com
**Professor, College of Engineering, Acharya Nagarjuna University, AP, India

Abstract: Mobile Ad hoc Networks (MANETs) has numerous security issues pertaining to dynamic topology. Specifically the issues of black hole and gray hole attacks which are more common impact the data transmission between the nodes, and needs significant solution to address such problems. In this paper, the proposal of a new model Node Eminence State and Node Sequence State based Route Discovery (NESSRD) for mobile ad hoc networks, towards addressing the identification and selection of route with nodes that are prone to attacks are proposed as an extension to the ENES model proposed earlier. The proposed solution works as heuristic in the selected route, and addresses the problems. The tests that are conducted under NS2 simulation, the results from the process signifies effective results in comparison to the CBDA model and the results are depicted in the study in detail along with the process adapted which depicts the robustness of NESSRD. The proposed model works on improving the scalability and in terms of detecting the black hole attack which could impact the nodes under minimal computational cost. The proposed model provides optimum performance in comparison to some of the earlier models reviewed in this paper and the results achieved under standard performance evaluation.

Keywords: NESSRD, Cooperative bait strategy, Node eminence score, black hole attacks, mobile ad hoc network (MANET).

Introduction

Mobile devices have become an integral part in the communication needs in the present. Apart from playing integral role in the critical communication system, even in the routine and generic communication too mobile devices has become an integral need. Usually the mobile ad hoc network is a pool of nodes and has no system of physical medium, and using the specific range of radio frequency, each node communicates with the other nodes. In such conditions, when one node has to transmit data to the other node in the out of range, there is need to establish a route between the nodes using and it is carried out by hop nodes.

As the network typology is dynamic in the case of node links, the routes are usually vulnerable to varied range of threats pertaining to data security and data loss related issues. Some of the significant issues are link failures, black holes, malevolent activities, and the selfish nodes, [1], [2], [3] that impact the process. In terms of establishing a secured route with the minimal process towards addressing the ad hoc networks [4] has become a prerogative.

In terms of routing protocols, some of them which are usually adapted are proactive, reactive and the hybrid ones which are adapted in the mobile and ad hoc networks. In terms of proactive strategy, the information exchange among the nodes are usually on the basis of routing topology defined at specific intervals, and leads to the process overhead, whereas in the case of the reactive strategy, the route shall be established only on demand, whereas in the reactive strategy, only when there is demand the routes are established.

Defending the black hole attack is more challenging in securing the dynamic routing,[4], [5], [6].In the black hole conditions, the compromised node initiates a forged route response with some kind of shortest path to destination, but the challenge is that is it leads to draining the transmitted packets before delivering it to the destination. There are numerous studies that are carried out on route discovery to address the issues of black hole attacks, and still the scope of work is on high demand.

Related Work

In the process of defending the malicious nodes, the proactive strategies adapted is to intimate the nodes about the compromised behavior of the nodes nearby [7-15]. One of the significant constraints in these models are about the act of collecting the topological status from the nearby nodes in regular intervals and it leads to performance issues of routing and resource utilization overhead and process overhead issues, categorically when the malicious nodes are absent. Though such limitations persists, still the proactive strategies support in preventing the role of malicious nodes at the initial stages,

whereas, in the reactive defense mechanisms, the inputs are detected in routing if any packet loss is identified in the process to the destination node. [16], [17], [18]. However, the key challenge with the defense mechanism is about the detection process initiation only after significant packet loss.

Liu et al [12] in their study depicts a proactive strategy towards addressing the malicious nodes in selected routes. Using the converse direction of the route, the two hop levels shall acknowledge in the packet transmission route, and such process of acknowledgment shall address issues pertaining to routing overhead, which is a key constraint in terms of proactive defense mechanisms.

Xue et al [16] proposed a reactive defense method as Best Effort Fault Tolerant Routing (BFTR), in which the acknowledgments from the destination node to source is the major process with inputs on the delivery ratio and delay. If any variance in the delivery ratio and the delay in the process observed, the source path chooses the alternate path to process the packets, and thus leading to route discovery process with recursive outcome resulting to process overhead.

T. Poongodi et al [19] proposed Localized Secure Routing Architecture that can work towards addressing the cooperative defensive black hole attacks. The proposed model of reactive strategy mainly depends upon the security monitoring node that can establish abnormal delay in the route due to black hole nodes. Though this system fine tunes the process, but still the constraint is about the malicious nodes involvement in the selected route.

In another study, the DNA-Based Cryptographic Mechanism [20] is proposed which handles the reactive strategy towards considerable process overhead, as a result of cryptographic standards that are used. Jian-Ming Chang et al [21] devised a Cooperative Bait Detection Approach (CBDA), which adapts the similar process towards the defending the collaborative attacks by the malicious nodes, and such reactive strategy reflects towards improving the process, but still there are many short come in terms of addressing the detection of malicious nodes in route discovery.

Focusing on the above set of solutions and the kind of scope for improvement that is envisaged in the process, the emphasis is on securing the route discovery strategy that can support in identifying optimal route addressing the issues of malicious attacks and improve the correspondence among the intermediate nodes. The proposed strategy is to focus on the Node Eminence State and Node Sequence verification (NESSRD) towards finding the secure route. The model has to depict the characteristics of proactive defense mechanisms that work with one time discovery of the topological state of the node. The proposed model NESSERD crosschecks the sequence currently used with the route response in the sequence of the nodes watched, unlike the security route discovery model adapted in CBDA.

The process is achieved by using the node eminence scope method as depicted in the earlier contribution ENES [22], by extending the search for node sequence state, towards identifying the malicious nodes in the optimal route discovery. The topological state in the nodes that are involved in the route shall have to be verified at the route selection by NESSRD. If any discrepancies are identified, only then the next optimal route shall be considered for node sequence state verification and optimal route discovery. The method of reactive defense strategies is identified in the proposed system.

The further sections of this paper reflect upon the proposed model in detail in the section -2 and the experimental study of the process is depicted in the section-3. Section-4 of this paper concludes the contributions made in the study.

Node Eminence State and Node Sequence State based Route Discovery

In the earlier contribution ENES, the process of estimating and updating the eminence scope of a node involved in ad hoc routing was depicted. [22], with limited set of metrics toward recognizing the selfish and under rated QoS factor nodes. To identify the black hole attack kind of intent in the nodes, the process of ENES shall be designed to perform additional process of node sequence state verification strategy. The simple process adapted by the system is to focus upon identifying the sequence of nodes between source and destination, and if any of the node is found to be artifact, then such node is marked as suspicious node, before further rating the route as prone to malicious. Upon finding the suspicious nodes from the respective router r, the route is decided as prone to malicious.. The following process is the method adapted for evaluation of nodes.

- Selection of Route

  Conditional broadcasting method shall be adapted for route selection

  Using the routing optimality ranking inputs, sequencing of the selected routes in descending order shall be implemented.
- Malicious route detection (see sec 3.2)
  1. Using the optimal route r from the response routes that are found in selection
  2. For each of the node n in the route,
     a. selection of the sequence of nodes found in the cached route $cr_{s\to n}$ between source node s and the node n
     b. if cached route $cr_{s\to n}$ is in existence and the sequence of nodes observed in $cr_{s\to n}$ is similar to sequence of nodes between s and n in r
        i. Inform the sequence of nodes between source node s and selected node n in the given route effective without risks of attacks.

c. Else if the node sequence between source and selected node is divergent between cached route and current route
    i. choose the nodes that are unique in the node sequence of the current route
    ii. Assess the transmission deflection ratio of the node is high, if high
        a. inform that the node sequence is suspicious (prone to attack)

End //end of 2

3. Found the similarity between the possible node sequences observed between source and all other nodes of the selected route and the suspicious node sequences. If identical nature is found to be more than 0, then route r is attack prone and continue the process 9step 2) to verify the next route discovered under route request strategy.
4. Else affirm the optimal route selected as safe route to transmit the data
5. Conduct the process of eminence update for all nodes involved in the selected route (see sec 3.3)

Route Discovery

By identifying all possible routes to transmit the data between the selected source and the destination node, using the qualified diffusion of the route request, the feasible routes to transmit the data from source to destination is identified he route request[18]. Let $R = \{r_1, r_2, ...r_{|R|}\}$ be the set of routes selected in route request process are chosen [18].

Assessing the current eminence score

ENES method is adapted in terms of evaluating the eminence scope for a node, and the following indicates the method of score calculation that is adapted in the process.

- 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 deflection 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:

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

Malicious Route Detection by Node Sequence State verification

The selected optimal route $\{r \exists r \in R\}$ is evaluated by node sequence state verification, and towards finding the suspicious route for each node $\{n \exists n \in r\}$, current recommended node sequence between source node s and selected node n will be assessed in terms of catching the node sequence for node s and node n.

In case of any variation identified among the lists, then average diffusion ratio between the current route and cached route is evaluated, along with the mean square error related to transmission diffusion identified for each of the route, identified with respective node. In the conditions where the mean square error is higher than the threshold defined and also the average diffusion rate for transmission is lower than the respective nodes, in such conditions, the node is confirmed for suitability. Also, if the mean square error is higher than the threshold alongside the average diffusion rate also being high, in such conditions, that node is marked as alternative choice.

In the other resulting cases, the respective node shall be classified as suspicious and is added to such list snl. Whether the route is prone to malicious attack is decided on the basis of all the nodes duly being evaluated. . 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. In the case of selected optimal route identified to be suspicious, in such conditions, the node sequence state verification shall be applied to the corresponding optimal route. $\{r \exists r \in R\}$.

The cyclic process is continued till the point of discovering a secure note from the route list R, and the metrics that are adapted in the model for decision are: (1) emphasis is on collecting the node sequence variation between catch nodes and current nodes. (2) Diffusion ratio is observed in current route but not in the catch route.
The algorithmic exploration of the node sequence state verification is as follows:
Let $snl \leftarrow \phi$ // an empty suspicious nodes list

1. $\underset{i=1}{\overset{|R|}{\forall}}\{r_i \exists r_i \in R\}$ Begin
   a. $\underset{j=1}{\overset{|r_i|}{\forall}}\{n_j \exists n_j \in r_i\}$ begin
   b. *if* $\left(\left\{cr_{s\to n} \exists cr_{s\to n} \in CRT_s\right\} \neq \phi\right)$ // selecting cached node sequence between source node s and node n of current route r
   c. *if* $(cr_{s\to n} \equiv r_{s\to n})$ // is the node sequence of node s and node n in cached route cr equals to the node sequence of node s and node n in current route r
      i. Node sequence of node s to node n found to be fair (no node in respective sequence is suspicious.
   d. Else
      i. $nnl \leftarrow \{r_{s\to n}\} \setminus \{cr_{s\to n}\}$ collecting the nodes that are exists in $r_{s\to n}$ and does not exists in $cr_{s\to n}$
      ii. $\underset{k=1}{\overset{|nnl|}{\forall}}\{n' \exists n' \in r_{s\to n} \wedge n' \notin cr_{s\to n}\}$
      iii. $atdr(n') = \dfrac{\sum_{p=1}^{|CRT|}\left\{tdr_{cr_p(n')} \exists n' \in cr_p\right\}}{\sum_{p=1}^{|CRT|}\left\{1 \exists n' \in cr_p\right\}}$ // average transmission diffusion ratio $atdr(n')$ of the node n' is estimating, $tdr_{cr_p(n')}$ is the transmission diffusion ratio (inverse of the ratio of ingress and egress load) observed for node n' under cached route cr_p. The transmission diffusion ratio of the node n' assessment explored in following equation
      $tdr_{cr_p(n')} = 1 - \dfrac{egr_{n'}}{igr_{n'}}$, which is the inverse of ratio between egress and ingress packet count observed for node n'
      iv. $rmse_{tdr(n')} = \dfrac{\sum_{p=1}^{|CRT|}\sqrt{\left(atdr(n') - \left\{tdr_{cr_p(n')} \exists n' \in cr_p\right\}\right)^2}}{\sum_{p=1}^{|CRT|}\left\{1 \exists n' \in cr_p\right\}}$
      // root mean square error $rmse_{tdr(n')}$ of transmission diffusion ratio observed at divergent cached routes is estimating.
      v. *if* $\left(\left(rmse_{tdr} < \tau_{rmse}\right) \wedge \left(atdr_{(n')} > \tau_{tdr}\right)\right)$
      //root mean square error $rmse_{tdr(n')}$ of transmission diffusion ratio observed at divergent cached routes is less than the given threshold τ_{rmse} and average transmission diffusion is more than the given threshold (this observations indicates the uniform and selective and high transmission diffusion, which is the property of gray hole attack).

      $snl \leftarrow n'$ // add node to suspicious nodes list snl

   e. End // end of d
   f. End //end of a
   g. $cn \leftarrow \{r_{s\to n}\} \cap \{snl\}$ // list of common nodes cn in route r_i and suspicious nodes list snl
   h. *if* $\left(|cn| \equiv 0\right)$ begin // if common nodes list is empty

i. Claim the r_i is secure and optimal route
j. Exit //exit the loop in 1
k. End // end of m

2. End // end of 1

Eminence Score Update

Once the routing process is completed, 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 that is identified in the case of data transmission over the router r. Also, the further level of eminence score is updated is completed using the following process.

Node n involved in the route r shall work on message for updating and corresponds to the successive node h that exists in the current route rt_i. Using the process of camouflage publishing approach for the node n, the encrypted form $ees(h)$ of the new eminence score $es(h)$ that XOR with a salt s. shall be adopted. In further process, signature $sig(h)$ of the node h indicating new eminence score will be generated and the confirmation message esu that contains $ees(n_i)$ and $sig(h)$ will be sent to node h.

In terms of restricting the scope of conditional acceptance, the scope for new eminence score in terms of 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 it shall be presented to the neighbor nodes. In a sequence, the further node h decrypts $ees(h)$ and then performs XOR operation on $es'(h)$ and s that results actual $es(h)$. Later node h updates its eminence score factors. Once the completion of updating the eminence score of node n_i is accomplished, source node informs $sig(n_i)$ to all other nodes by adapting broadcasting strategy.

Experimental Study

In terms of performance evaluation, NESSRD shall be tested in multiple dimensions, like the traditional route performance assessment metrics, leading to “ratio of packet delivery” and “delay” in which the inputs are analyzed and in the other form, accuracy in terms of detecting the malicious node and sensitivity were also assessed towards determining the process of nodes discovery and the related factors which shall support in identifying the node sequence verification. (see sec 3.2).Outcome that is achieved in the process were also compared the other model of CBDA [21], for performance evaluation. Analysis is carried out using a system with configuration of 4GB ram and i5 processor, for evaluating the routing performance. NS2 services were used towards assessing the routing performance, using the simulation of the mobile ad hoc network. The specifications that are used towards addressing the simulation in the network are depicted in the table 1. By using the explorative language R, the malevolent node detection accuracy and sensitivity analysis has been assessed.

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

In the case of delays that are observed in CBDA, the performance is inconsistent at the ration levels of 0.08, but in terms of delay depicted at higher ration of malicious nodes (0.12, 0.16 and 0.2) are relatively higher than what is depicted in the case of NESSRD. The linearity that is resulting from NESSRD in the tests, pertaining to relay, reflects upon malicious nodes. (see fig 1).

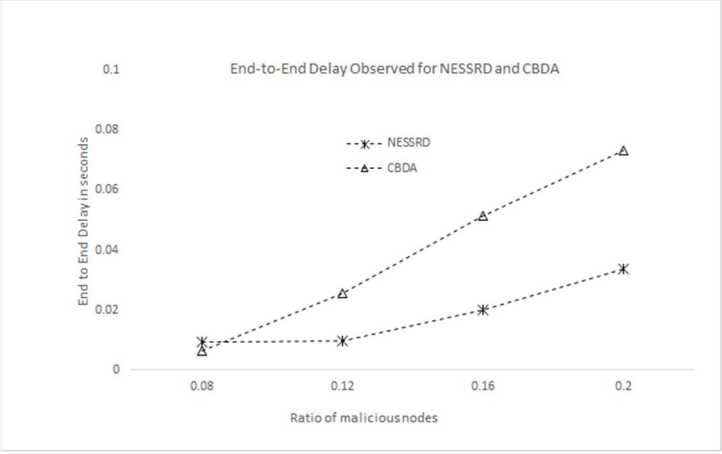

Figure 1: The end to end delay observed for NESSRD and CBDA

Figure 2 indicates the dwindling performance of CBDA towards managing the optimal packet delivery ratio, with varied ration of malicious nodes that could be assessed in terms of NESSRD. In NESSRD, the stability that is reflected in optimal avoidance of the malicious nodes towards route discovery with proposed node sequence state verification strategy(see fig 2).

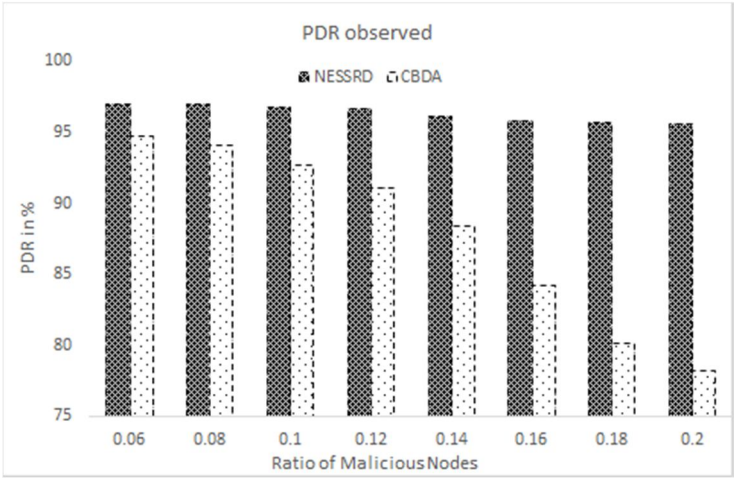

Figure 2: The Packet Delivery Ratio observed for NESSRD and CBDA

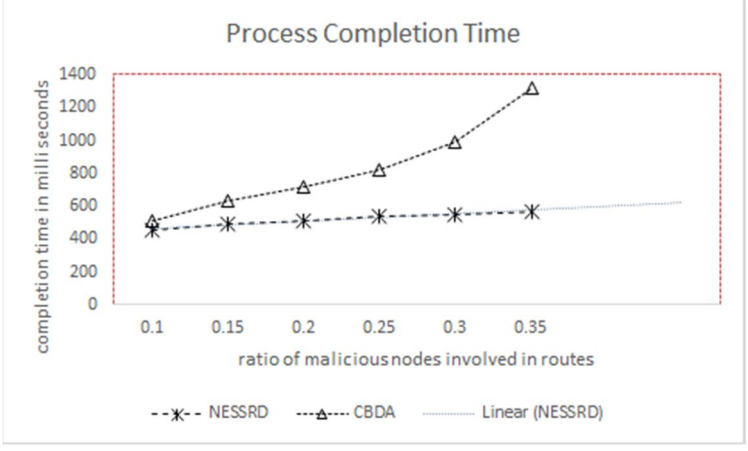

Figure 3: Completion time observed for divergent ratio of malicious nodes involvement in input routes

In terms of evaluating the normal and malevolent nodes, the process of assessment is carried out using 28 malicious nodes and 145 normal nodes that shall be used for statistical assessment, for related accuracy and sensitivity. Taking cue of input routes, classification of nodes as true-positives, true-negatives, false-positives and false-negatives has been categorized for the labels by NESSRD and CBDA. Also, in terms of process complexity which is observed in the NESSRD, there is linear (see the fig 3), which depicts that the model NESSRD is scalable and robust.

Conclusion

This paper depicts an effective solution towards addressing the issues pertaining to defending the role of black-hole and gray-hole nodes that could make significant importance to the discovery of mobile ad hoc network. Proposed model is termed as Node Eminence State and Node Sequence State Verification based secure route discovery, constituting the characteristics of both proactive and reactive defense mechanisms. In comparison to usual proactive defense mechanisms, in which the observation of topological state of the neighbor nodes with periodical intervals are high, in the proposed model, the response routes are estimated only once during the optimal route selection process, thus leading to more effective performance of the system. But the challenge is about not considering the process overhead issues of the proactive mechanisms, and as a result only when the routes found with black hole node involvement, the bait strategy is adapted to identify the black hole nodes, as similar to defense mechanism. From the results of experimental study, it is imperative that the process is very resourceful and effective compared to the CBDA model. In terms of future direction, it can be stated that focus could be on defending malicious acts like the vampire attacks and improving the operational efficiency of the system by improving the route discovery process with minimal computational complexity.

References

[1] Zhou, Lidong, and Zygmunt J. Haas. "Securing ad hoc networks." IEEE network 13.6 (1999): 24-30.
[2] Zapata, Manel Guerrero, and Nadarajah Asokan. "Securing ad hoc routing protocols." Proceedings of the 1st ACM workshop on Wireless security. ACM, 2002.
[3] Papadimitratos, Panagiotis, and Zygmunt J. Haas. "Secure message transmission in mobile ad hoc networks." Ad Hoc Networks 1.1 (2003): 193-209.
[4] Hu, Yih-Chun, and Adrian Perrig. "A survey of secure wireless ad hoc routing." IEEE Security & Privacy 2.3 (2004): 28-39.
[5] Sanzgiri, Kimaya, et al. "A secure routing protocol for ad hoc networks."Network Protocols, 2002. Proceedings. 10th IEEE International Conference on. IEEE, 2002.
[6] Deng, Hongmei, Wei Li, and Dharma P. Agrawal. "Routing security in wireless ad hoc networks." IEEE Communications magazine 40.10 (2002): 70-75.
[7] Chang, Jian-Ming, et al. "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture."Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on. IEEE, 2011.
[8] Corson, Scott, and Joseph Macker. Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations. No. RFC 2501. 1998.
[9] Baadache, Abderrahmane, and Ali Belmehdi. "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks." arXiv preprint arXiv:1002.1681 (2010).
[10] Marti, Sergio, et al. "Mitigating routing misbehavior in mobile ad hoc networks." Proceedings of the 6th annual international conference on Mobile computing and networking. ACM, 2000.
[11] Vishnu, K., and Amos J. Paul. "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks." International Journal of Computer Applications 1.22 (2010): 38-42.
[12] Liu, Kejun, et al. "An acknowledgment-based approach for the detection of routing misbehavior in MANETs." IEEE transactions on Mobile Computing6.5 (2007): 536-550.
[13] Deng, Hongmei, Wei Li, and Dharma P. Agrawal. "Routing security in wireless ad hoc networks." IEEE Communications magazine 40.10 (2002): 70-75.
[14] Ramaswamy, Sanjay, et al. "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks." International conference on wireless networks. Vol. 2003. 2003.
[15] Weerasinghe, Hesiri, and Huirong Fu. "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation." Future generation communication and networking (fgcn 2007). Vol. 2. IEEE, 2007.
[16] Xue, Yuan, and Klara Nahrstedt. "Providing fault-tolerant ad hoc routing service in adversarial environments." Wireless Personal Communications29.3-4 (2004): 367-388.
[17] Kozma, William, and Loukas Lazos. "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits." Proceedings of the second ACM conference on Wireless network security. ACM, 2009.
[18] Wang, Weichao, Bharat Bhargava, and Mark Linderman. "Defending against collaborative packet drop attacks on MANETs." 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009)(in Conjunction with IEEE SRDS 2009), New York, USA. Vol. 27. 2009.
[19] Poongodi, T., and M. Karthikeyan. "Localized Secure Routing Architecture Against Cooperative Black Hole Attack in Mobile Ad Hoc Networks."Wireless Personal Communications: 1-12.

[20] Babu, E. Suresh, C. Nagaraju, and MHM Krishna Prasad. "Efficient DNA-Based Cryptographic Mechanism to Defend and Detect Blackhole Attack in MANETs." Proceedings of International Conference on ICT for Sustainable Development. Springer Singapore, 2016.
[21] Chang, Jian-Ming, et al. "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach." IEEE systems journal 9.1 (2015): 65-75.
[22] G. Soma Sekhar and E. Sreenivas Reddy. "ENES: Exploratory Node Eminence State for Secure Routing in Mobile Ad hoc Networks."International Journal of Applied Engineering Research 11.8 (2016): 5863-5868.
[23] Ihaka, Ross, and Robert Gentleman. "R: a language for data analysis and graphics." Journal of computational and graphical statistics 5.3 (1996): 299-314.