Asian Journal of Information Technology 13 (4): 200-206, 2014
ISSN: 1682-3915

Cornbach Alpha Coefficient Based Trust Model for Routing in MANET

[1]S. Pariselvam and [2]R.M.S. Parvathi
[1]Manakula Vinayagar Institute of Technology, Puducherry, India
[2]Senguthar College of Engineering, Thiruchengode, Namakal District, Tamil Nadu, India

Abstract: Fill the text co-operation is considered as one of the important factor that has a vital influence in the reliable data dissemination of packets between the wireless nodes present in an ad hoc scenario. This co-operation is also essential for maintaining both the forward and reverse routes between the source and the sink nodes. Due to the stringent availability of resources in MANETs, some of the participating nodes present in the ad hoc environment may exhibit a malicious behavior of intentionally dropping the data packets rather than forwarding to their neighbor nodes. This maliciousness of the nodes may result in the degradation in the network performance. In this study, researchers formulate and propose a Cornbach alpha coefficient based trust model which manipulates the trust of each and every node present in the topology based on Cornbach alpha coefficient. The experimental analysis of the proposed trust model is studied through the ns-2 simulation with the aid of evaluation parameters namely packet delivery ratio, control overhead, total overhead and throughput by varying the number of malicious nodes. This proposed scheme performs well when compared to the model present in the literature like split half reliability model.

Key words: Cornbach alpha coefficient, malicious node, MAODV, trust model, reliability model

INTRODUCTION

Form the recent past, most of the researchers had not explored the concept of Co-operation as a critical entity that has to maintained between the nodes present in a MANET environment (Buchegger and Le Boudec, 2003). This research issue is considered as very vital because, MANETs are dynamic in nature and they lack a common centralized infrastructure. If the node in the ad hoc environment behaves in a malicious manner, then the performance of the network degrades (Michiardi and Molva, 2002). Therefore, a trust model becomes more vital for monitoring the nodes behavior. The literature survey has proved that the reliability coefficients could analyze the he statistical data more appropriately when compared to the other available consistency check mechanisms (Mei and Stefa, 2012).

In this proposed research, researchers formulate a Cornbach Alpha Coefficient based Trust Model (CACTM) for determining the trust of each and every nodes present in an ad scenario. MAODV is the multicast protocol used for our simulation study. The protocol makes use of RREQs. RREPs, MACT and GRPH as the control packets for establishing communication between the nodes present in the topology. Researchers employ the group communication between the nodes in order to study the impact of malicious present during group communication. The simulation study was carried out to compare the proposed CACTM Model with the SHRCM Model based on the evaluation parameters namely packet delivery ratio, control overhead, total overhead and throughput by varying the number of the mobile nodes deployed for group communication.

Existing research: In the past decade exhaustive research has been carried out for the enforcement of the cooperation among the mobile nodes in the MANET by detection and isolating or mitigating the non-cooperating, malicious nodes. This detection and isolation process is done based on two different techniques. Some of the researches are presented.

Mei and Stefa (2012) presented a reputation mechanism which is implemented by means of the technique known as force faithful technique. This technique works based on the assumption that in the given protocol strategy that there is not even a single node deviates from the cooperation. This technique reduces the number of duplicates which in turn considerably reduces the storage requirements thereby improving the network performance.

Eidenbenz *et al*. (2008) proposed a distributed framework which predicts the reliability of the mobile

Corresponding Author: S. Pariselvam, Manakula Vinayagar Institute of Technology, Puducherry, India

nodes. This framework is implemented with the four different basic constrains for the computation of the reliability of the mobile node. The constrains are a mobile node must motivate the routing process by means of its cooperation, the coordination given by the mobile nodes must be truthful, the routing process of the MANET must be in such a way that the packets has to be send through energy efficient path, the message transmission complexity regarding the intimation of malicious nodes in the MANET must be very less. The proposed methodology also implements game theory technique to improve the performance of the network.

Refaei *et al.* (2005) proposed a second hand reputation mechanism which continuously monitors its neighbor nodes in the ad hoc network. In this each and every node is implemented with reputation evaluation mechanism by means of maintaining the reputation index and reputation table. For each successful delivery of a node, the reputation index value gets incremented and updated in the reputation table. This study proposes three heuristic search methods for making decisions from the obtained values of packet delivery rates of each and every node. The heuristics methods are based on number of hops away form the source, single augmentation and double augmentation, the early probation.

Li and Shen (2012) presented a second hand reputation mechanism which makes use of reputation values computed by the neighbors of the mobile nodes. In this, researchers also derives a threshold value to obtain effective discrimination of the non corporation, non trustworthy nodes from the normal node in the MANET. This study also comes up with an integrated approach for detecting and mitigating selfish nodes. This is implemented based on game theory which investigates the network performance.

Li and Wu (2010) modeled an algorithm based on dynamic Bayesian signaling game for the improving the cooperation among the mobile nodes in ad hoc network. This mechanism discriminates the nodes based on the behavior of normal nodes and a malicious node by means of continues monitoring of each and every node by its neighbors. This is implemented by means of the concepts like sequential rationality and random property.

Abd Razak *et al.* (2008) addressed friendship mechanism for the enhancement of the cooperation of the mobile nodes by optimizing the resources. The reduction of false positives, i.e., incorrect identification of the selfish nodes can be reduces considerably. This method is implemented in two different methodologies viz., direct and indirect friend indirect mechanism. In this, researchers have also analyzed the various aspects of separation in terms of six degrees and also suggested solutions to get fid of all types of separation. They also implemented a voting strategy for discriminating malicious node from normal node.

Inaltekin and Wicker (2008) analyzed different problem that arise while achieving cooperation among the mobile node in ad hoc networks. Researchers have proposed levesque measure based on game theory which derives the probability values of all the nodes participating in the communication. In this, behavior of network is also analyzed based on equilibrium function.

Types of reliability coefficients available for computing the trust of nodes in an ad hoc scenario: A number of reliability coefficients are available in the literature that could be helpful in determining the trust of the node present in the ad hoc environment. Some of the reliability coefficients are discussed in this study.

Split half reliability coefficient: This kind of reliability coefficients are mainly suited in an environment where the behavior of the nodes are monitored based on large scale data. This coefficient provides better accuracy in manipulating the reliability of the nodes rather than making an understating or over estimation on the reliability of the nodes (Sengathir and Manoharan, 2013).

Kuder-Richardson coefficient: These kind of reliable coefficients are mainly ideal in a scenario when the behaviors of the mobile are analyzed based on dichotomous outcomes determined. But this coefficient provides does not provide higher degree of accuracy and reliability while compared to Cornbach alpha coefficient (Gliem and Gliem, 2003)

Regression coefficient: In this coefficient computation method, the degrees of deviation in between the number of incoming packets to the number of outgoing packets are considered as vital. Higher the regression value infers that the node has high possibility of behaving in a malicious manner (Dressal, 1999).

Literature review: The schema available in the literature for computing the trust level of the node, so that their isolation may aid in increasing the throughput of the network has some of the pitfalls as enumerated. They are:

- A reliability coefficient based trust model incorporating two levels of trust manipulation has not been proposed

- A methodology which could identify the presence of malicious nodes based on the Cornbach alpha coefficient which is based on the cumulative sum of incoming packets to the cumulative sum of outgoing packets has not been explored

These are the motivational factors for the formulation of a detection mechanism that helps in detecting the malicious nodes for preventing the network from degradation based on the computation of correlated Cornbach reliability coefficient.

MATERIALS AND METHODS

Cornbach alpha coefficient based trust model: In this study, researchers depict a Cornbach alpha coefficient based trust model formulated for identifying and isolating malicious nodes present in an ad hoc scenario. In this model, the detection is mainly innovated through a parameter called Cornbach alpha coefficient which is manipulated similar to that of Kudar Richardson coefficient. Suppose, researchers consider the sum of packets relayed by a nodes n for k sessions, then for $X = y_1+y_2+...+y_n$. Cornbach α is defined by the Eq. 1:

$$\alpha = \frac{k}{k\text{-}1}\left(1-\sum_{i=1}^{k}\frac{\sigma n_i^2}{\sigma n^2}\right) \quad (1)$$

Where:

σn^2 = The variance in the packet arrival rate for the total session k

σn_i^2 = The variance of packet delivery for each session k

Furthermore, the variance of σn can be calculated based on Eq. 2:

$$\sigma n = \frac{\sum (x_i-\bar{x})^2}{k\text{-}1} \quad (2)$$

where the variance sum of deviation $\sum_{i=1}^{k}\sigma n_i^2$ for each session can be computed as Eq. 3:

$$\sigma n_i^2 = \sigma n_1^2+\sigma n_2^2+\sigma n_3^2+...+\sigma n_u^2 \quad (3)$$

Here:

$$\sigma n_i = dev\,(x_i-x_r) \quad (4)$$

dev (x_i-x_r) is the deviation in the packet delivery rate for each session k. Furthermore, the node trust can be recomputed by the Eq. 5:

$$ST_{CAL} = \frac{K\bar{Z}}{(1+(k\text{-}1)E)} \quad (5)$$

where, Z is the mean of the k (k-1)/2 non reduction deviation co-efficient. The obtained ST_{CAL} detects that the node is malicious or not.

Cornbach alpha coefficient based trust model for MAODV routing:

Notations:

SRC: Source Node

DSG: Destination group of nodes

T_{CAC}: Trust based Cornbach alpha coefficient

1. The SRC floods the packets through all possible routes
2. The DSG acknowledges with the help of RREP through reverse routes
3. SRC forward data to DSG through optimal path based on multicast group id
4. The adjacent neighbor nodes of each and every node are mentioned for manipulating the variance in packets for entire k sessions as well as for each session
5. Then, monitoring neighbor nodes by computing T_{CAC} with the help of Eq. 1-3
6. If ($T_{CAC} \leq 0.3$) then
7. The node is malicious node
8. Call isolate();
9. Else
10. The node exhibits normal behavior.
11. The monitoring nodes again recompose the trust of each node monitored through ST_{cac}
12. If ($ST_{cac} \leq 20$)
13. Then, the neighbor conforms the node distrusts
14. Else
15. End if

In a MAODV protocol, the source node broadcasts the RREPs to all feasible paths to the group of nodes. The group of nodes identified by its Multicast Activation Packet (MACT) and GRPH replies by sending RREP through the reverse routing. Each and every nodes are monitored by their neighbors and they manipulate T_{CAC} (Trust based Cornbach Alpha Coefficient) which is based on the variation of packets for entire k sessions as well as each and every session. If this parameter is ≤ 0.3 then the node can be conformed as distrust or malicious node. Again, the neighbor node reconfirms their monitored node's distrust by calculating the coefficient called ST_{CAC}. When ST_{CAC} is ≤ 0.20 then it is isolated.

Illustration of proposed research: In this study, researchers portray a Cornbach alpha coefficient based trust model for detecting and isolating distrust nodes. This could be established through the manipulation of two coefficients T_{CAC} and St_{CAC}. For instance consider group of nodes in MANET on MAODV protocol as shown in Fig. 1.

Suppose if researchers consider the node B as the monitored node by their neighbors S, C and D based on the deviation in number of packets for each session and overall sessions. Then, monitoring neighbor nodes compute the value of T_{CAC}. If this parameter is ≤ 0.3

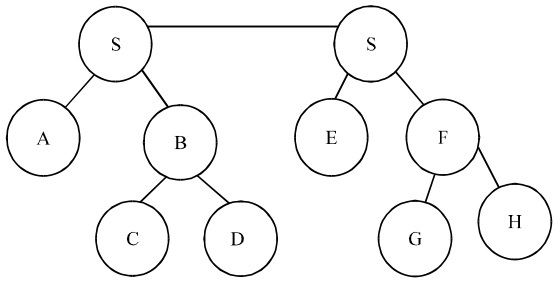

Fig. 1: Group of mobile nodes in MAODV protocol

then the node can be conformed as distrust or malicious node. Again, the neighbor node reconfirms their monitored node's distrust by calculating the coefficient called ST_{CAC}. When ST_{CAC} is ≤0.20, then the node B is isolated because of its maliciousness.

RESULTS AND DISCUSSION

The experimental simulations of the research in an extensive manner with the aid of network simulator tool ns-2.26. The experimental setup consists of 50 mobile nodes deployed in the maximum terrain size of 1000×1000 m^2. The experimental results were determined based on the cumulative sum of 10 simulation rounds. The optimal number of packets utilized for carrying out the simulation study is 1000 which could be feasible to perform the entire rounds of simulation. The 1 sec is considered as the refresh interval. The wireless channel capacity and the maximum size of the packet transmitted from the source node are 1 Mbp and 512 bytes, respectively.

Evaluation metrics: The thorough experimental analysis of the formulated Cornbach Alpha Coefficient based Trust Model (CACTM) is performed based on the following evaluation parameters.

Packet delivery ratio: It is defined as the ratio of the total number of packets forwarded for the neighbors to the total number of packets actually received from the neighbors within the simulation time.

Control overhead: It may be defined as the optimal number of bytes of packets that cold be utilized for establishing effective communication between the source nodes and the sink nodes.

Total overhead: It may be defined as the ratio between the total number of control and data packets destined to the destination nodes to the actual number of data packets delivered to those destination nodes.

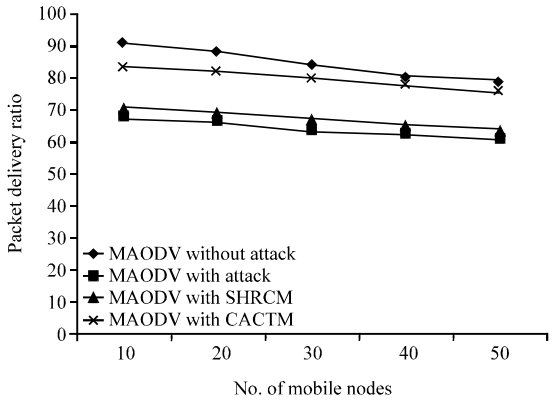

Fig. 2: Performance analyses for packet delivery ratio based on CACTM by varying the number of mobile nodes

Table 1: Simulation parameters

General parameters	Values
Number of nodes	50
Type of protocol	MAODV
Simulation time	2000
MAC layer	802.11
Range of transmission	300 m
Simulation area	1000×1000 m^2
Traffic model parameter	
Traffic model	Constant bit rate
Packet size	512 bytes
Interval	1 sec
Type of antenna	Antenna/Omni antenna
Type of propogation	Two ray ground
Type of interface queue	Queue/Drop tail/Priority queue

Throughput: It may be defined as the aggregate number of packets that reaches the sink node from the source node within the simulation time t. The simulation tables containing various parameters set for the experimental study are depicted with the help of Table 1.

Performance Evaluation for Cornbach Alpha Coefficient based Trust Model (CACTM)

When the number of malicious nodes (n = 10) (Packet delivery ratio): The performance of the ad hoc network highly depends on the number of malicious nodes n when routing is performed with the help of MAODV protocol. The packet delivery ratio decreases based on the number of the malicious nodes present in the ad hoc scenario. Hence, the need arises for the deployment of trust based schema like CACTM. From Fig. 2, it is obvious that the implementation of CACTM in the MAODV protocol shows a steady increase in performance in terms of packet delivery ratio when compared to the existing model like SHRCM. This proposed model CACTM shows a phenomenal increase of 27% in packet delivery ratio.

Control overhead: The presence of malicious nodes in an ad hoc scenario increases the number of retransmission

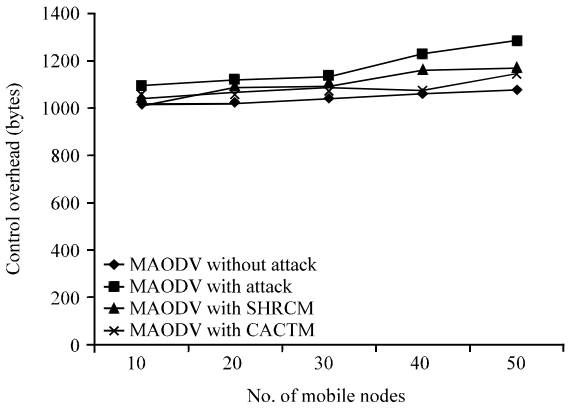

Fig. 3: Performance analysis for control overhead based on CACTM by varying the number of mobile nodes

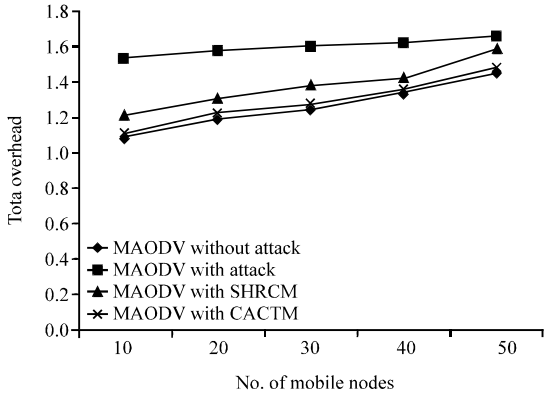

Fig. 4: Performance analysis for total overhead based on CACTM by varying the number of mobile nodes

resulting in the control packet overhead. Hence, the control overhead has to reduce phenomenally to increase the performance of the network when routing is carried with the aid of MAODV protocol. From Fig. 3, it is obvious that the deployment of CACTM in the MAODV protocol shows a steady decrease in the control overhead when compared to SHRCM.

Total overhead: The total overhead increases when the number of malicious nodes present in the ad hoc environment increases. Since, the performance of the network is based on lower total overhead while routing is carried with MAODV. Thus, the need for the implementation of trust schema like CACTM arises. From Fig. 4, it is obvious that deployment of CACTM in the MAODV protocol shows a steady decrease in the total overhead when compared to SHRCM. This proposed model CACTM shows a phenomenal decrease of 19% in total overhead.

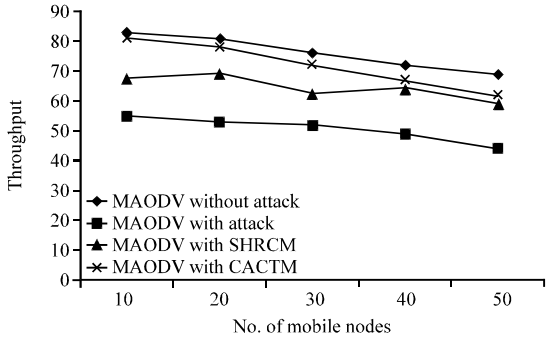

Fig. 5: Performance analysis for throughput based on CACTM by varying the number of mobile nodes

Throughput: The throughput of the entire network depends on the reliable data dissemination between the source and the sink. But the presence of the malicious nodes may decrease the performance of the network in terms of throughput. Therefore, when a trust based model like CACTM is implemented there is steady increase in throughput. From Fig. 5, it is obvious that the deployment of CACTM in the MAODV protocol exhibits a phenomenal increase in the network throughput.

When the number of malicious nodes (n = 20)

Packet delivery ratio: The performance of the ad hoc network highly depends on the number of malicious nodes n when routing is performed with the help of MAODV protocol. The packet delivery ratio decreases based on the number of the malicious nodes present in the ad hoc scenario. Hence, the need arises for the deployment of trust based schema like CACTM. From Fig. 6, it is obvious that the implementation of CACTM in the MAODV protocol shows a steady increase in performance in terms of packet delivery ratio when compared to the existing model like SHRCM. This proposed model CACTM shows a phenomenal increase of 29% in packet delivery ratio.

Control overhead: The presence of malicious nodes in an ad hoc scenario increases the number of retransmission resulting in the control packet overhead. Hence, the control overhead has to reduce phenomenally to increase the performance of the network when routing is carried with the aid of MAODV protocol. From Fig. 7, it is obvious that the deployment of CACTM in the MAODV protocol shows a steady decrease in the control overhead when compared to SHRCM.

Total overhead: The total overhead increases when the number of malicious nodes present in the ad hoc

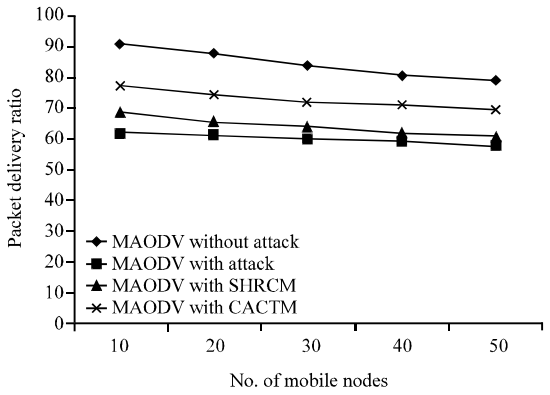

Fig. 6: Performance analysis for packet delivery ratio based on CACTM by varying the number of mobile nodes

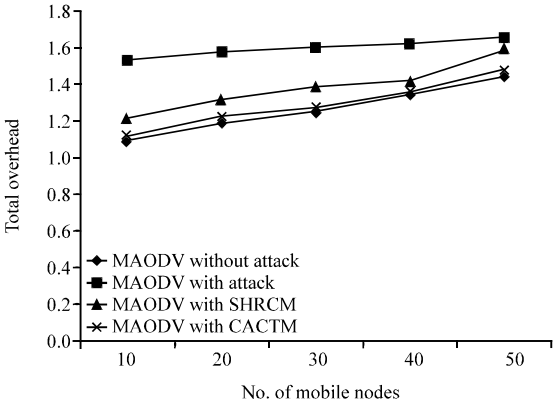

Fig. 8: Performance analysis for total overhead based on CACTM by varying the number of mobile nodes. CACTM shows a decrease in throughput

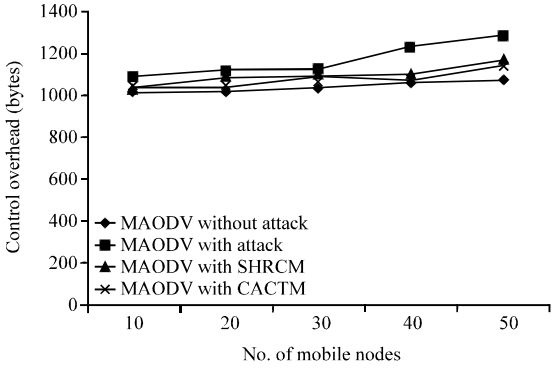

Fig. 7: Performance analysis for control overhead based on CACTM by varying the number of mobile nodes. CACTM shows a decrease in control overhead

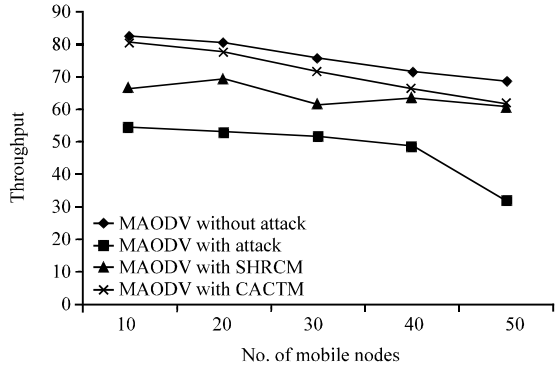

Fig. 9: Performance analysis for throughput based on CACTM by varying the number of mobile nodes. CACTM shows a phenomenal increase in throughput

environment increases. Since, the performance of the network is based on lower total overhead while routing is carried with MAODV. Thus, the need for the implementation of trust schema like CACTM arises. From Fig. 8, it is obvious that deployment of CACTM in the MAODV protocol shows a steady decrease in the total overhead when compared to SHRCM.

Throughput: The throughput of the entire network depends on the reliable data dissemination between the source and the sink. But the presence of the malicious nodes may decrease the performance of the network in terms of throughput. Therefore, when a trust based model like CACTM is implemented there is steady increase in throughput. From Fig. 9, it is obvious that the deployment of CACTM in the MAODV protocol exhibits a phenomenal increase in the network throughput. This proposed model CACTM shows a phenomenal increase of 26% in throughput.

CONCLUSION

In this study, a Cornbach alpha coefficient based trust model proposed makes it clear that this trust based schema outperforms the existing trust based model like split half reliability model in terms of packet delivery ratio, control overhead, total overhead and throughput. In this proposed model, the nodes make its decision based on the Cornbach α coefficient in a distributed manner. In the near future, the proposed research can further analyze based upon the scalability and resilience factors of the network. This proposed model CACTM shows a phenomenal average increase of 20% in packet delivery ratio, control overhead, total overhead and throughput.

REFERENCES

Abd Razak, S., N. Samia and M.A. Maarof, 2008. A friend mechanism for mobile ad hoc networks. Proceedings of the 4th International Conference on Information Assurance and Security, September 8-10, 2008, Naples, Italy, pp: 243-248.

Buchegger, S. and J.Y. Le Boudec, 2003. A robust reputation system for mobile ad-hoc networks. EPFL IC Technical Report IC/2003/05. http://infoscience.epfl.ch/record/486/files/IC_TECH_REPORT_200350.pdf.

Dressal, P., 1999. Some remarks on the Kuder-Richardson reliability coefficient. Phychometrica, 8: 223-245.

Eidenbenz, S., G. Resta and P. Santi, 2008. The commit protocol for truthful and cost-efficient routing in Ad hoc networks with selfish nodes. IEEE Trans. Mobile Comput., 7: 19-32.

Gliem, J.A. and R.R. Gliem, 2003. Calculating, interpreting and reporting Cronbach's alpha reliability coefficient for likert-type scales. Proceedings of the Midwest Research-to-Practice Conference in Adult, Continuing and Community Education, October 8-10, 2003, The Ohio State University, Columbus, OH., USA., pp: 82-88.

Inaltekin, H. and S.B. Wicker, 2008. The analysis of Nash equilibria of the one-shot random-access game for wireless networks and the behavior of selfish nodes. IEEE/ACM Trans. Networking, 16: 1094-1107.

Li, F. and J. Wu, 2010. Attack and flee: Game-theory-based analysis on interactions among nodes in MANETs. IEEE Trans. Syst. Man Cybernet. Part B: Cybernet., 40: 612-622.

Li, Z. and H. Shen, 2012. Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks. IEEE Trans. Mobile Comput., 11: 1287-1303.

Mei, A. and J. Stefa, 2012. Give2Get: Forwarding in social mobile wireless networks of selfish individuals. IEEE Tras. Dependable Secure Comput., 9: 569-582.

Michiardi, P. and R. Molva, 2002. CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. Proceedings of the IFIP TC6/TC11 6th Joint Working Conference on Communications and Multimedia Security, September 26-27, 2002, Portoroz, Slovenia, pp: 107-121.

Refaei, M.T., V. Srivastava and L. DaSilva, 2005. A Reputation-based mechanism for isolating selfish nodes in ad hoc networks. Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, July 17-21, 2005, London, UK., pp: 3-11.

Sengathir, J. and R. Manoharan, 2013. A split half reliability coefficient based mathematical model for mitigating selfish nodes in MANETs. Proceedings of the IEEE 3rd International Advance Computing Conference, February 22-23, 2013, Ghaziabad, India, pp: 267-272.