WULFENIA JOURNAL
KLAGENFURT, AUSTRIA ISSN:1561-882X

Vol 21, No. 3;Mar 2014

Manifestation and Mitigation of Node Misbehaviour In Adhoc Networks

Burhan Ul Islam Khan[1,a] , Rashidah F. Olanrewaju[2,b], Farhat Anwar[3,c] and Asadullah Shah[4,d]

[1,2,3]Department of Electrical and Computer Engineering, Kulliyyah of Engineering, International Islamic University Malaysia

[4]Department of Computer Science, Kulliyyah of Information and CommunicationTechnology, International Islamic University Malaysia

[a]burhan.iium@gmail.com, [b]frashidah@iium.edu.my, [d]asadullah@kict.iium.edu.my, [c]farhat@iium.edu.my

Abstract— Mobile adhoc network is signified as a boon for advance and future wireless communication system. Owing to its self-establishing network features and decentralization, the system can actually establish a wireless communication with vast range of connectivity with the other nodes. However, the system of MANET is also beheld with various technical impediments owing to its inherent dynamic topologies. Although there are abundant volume of research work, but very few have been able to effectively address the node misbehavior problems in MANET. The paper initially tries to draw a line between different types of nodes in MANETs based on their behavior characteristics, then reviews some of the significant contribution of the prior researches for addressing node misbehavior issues. A major emphasis is laid on is the researches which use game theory as a tool to study and address the misbehavior problems. The manuscript is developed considering some of the latest and standard evidences of past 5 years and finally discusses the open issues related to the problems.

Keywords-component: Mobile Adhoc Network, Selfish Node, Malicious node, Node Misbehaviour.

I. Introduction

A mobile adhoc network or popularly known as MANET has been the constant focus of the research community due to its potential communication capability using mobile devices. In MANET, the mobile device acts itself as an individual router and thereby tends to move in independent direction. Owing to dynamic topology of nodes all the QoS issues as well as security issues arise in MANET. Although, various QoS issues e.g. bandwidth, latency, packet delivery ratio, etc. has witnessed an extensive study in the past, but security problems inevitably are yet to see the some standard and remarkable outcome. Due to dynamic topology, such adhoc network encounters frequently intermittent link that affects the communication immensely. Owing to the decentralized nature of the network, MANET security system poses a higher dimensional challenging with respect to authentication and authorization. One of the complex security problems in MANET is to visualize the behaviour of node, which may be any type of computing devices e.g. laptop, tablet PC, smart-phone etc. Various literatures (Belding et al., 2004), (Makki et al., 2007) explored that MANET possesses 4 types of nodes viz. i) regular node, ii) erroneous node, iii) selfish node, and iv) malicious node. A regular node is the one which is interested to establish communication with other node for the purpose of forwarding a data packet. Erroneous node is the one with circuitry issues and defective hardware design that potentially poses as an impediment for security protocols as well as for enabling reliable communication. Whereas selfish node tends to refuse to forward the data packet to the destined nodes in order to save its resources, while malicious nodes always keeps harmful intention to disrupt the traffic and steal the confidential data. Fig.1 shows the communication model and node classification in MANET.

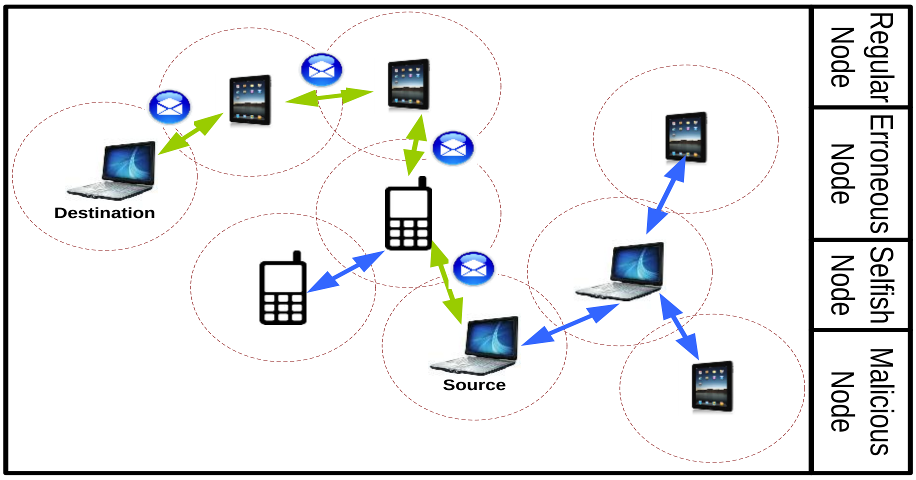

Figure 1 Types of node in MANET

Literatures have essentially surveyed the various types of attacks in MANET along with countermeasures, but it is yet to be seen which one is more effective. Various cryptographic based studies have been conducted in the past to provide better security. However, more or less every prior study considers certain case study of attack scenario and then deploys formulation of attack mitigation model. One of the disadvantage of such study is that the countermeasures techniques are highly specific and is not applicable when the adversarial scenario changes. Hence, it is important that before formulating a new mitigation technique against the security issues of MANET, the node misbehavior problems should be investigated properly as it is one of the complex studies. Understanding the behaviour of various kinds of nodes in a MANET system will enable the researcher to closely visualize the pattern of attacks and attacking strategy. It will also assist the researcher to visualize how far their mitigation technique will be successful on a selected attack scenario. Hence, better security protocol can be designed cost effectively if the exact behaviour of the node be extracted empirically. Hence, the proposed study reviews some of the potential literatures in the past that have studied the traits of node misbehavior. The study will also excavate contribution of the game theory for the similar purpose, and finally open issues are discussed. Section 2 describes node misbehavior problem in MANETs with its causes and imperious security concerns followed by Section 3 highlighting the researches aimed at tackling the same. Section 4 exclusively discusses about the game theoretic approach as a mitigation technique to thwart node misbehavior followed by brief discussion on open issues in Section 5. Finally, Section 6 summarizes the cumulative findings of the paper.

II. UNDERSTANDING NODE MISBEHAVIOR

One of the critical demerits of MANET system is its decentralization as well as its ongoing node mobility which consumes unwanted power and decision of routing protocol thereby posing a great challenging task. Due to this unwanted power drainage as well as limitation of channel capacity, there are some groups of nodes that may choose to reject forwarding or carrying any request from its neighborhood nodes due to its resource constraint. Such nodes are basically termed as Erroneous Nodes (Yang et al., 2004) which rises due to technical issues of power or software/hardware problems. Existence of such nodes can be easily taken advantages by the malicious node which will always have certain harmful intention in order to paralyze the operational aspects of MANET system. However, there is a presence of other types of node in MANET which majorly imitates the behavior of Erroneous Node called as selfish node (Schutte, 2006).

The characteristics adopted by selfish nodes target to gain the benefit of network at the cost of other node resources opportunistically. Selfish nodes do not take part in packet forwarding and they are considered to behave very much rationally as they act opportunistically to gain network resources as advantages. Hence the presence of selfish node is potentially harmful as the similar behavior of the selfish node can be easily imitated by malicious node, which is the point of concern of many security aspects. As there is no presence of integrated digital certificate based node verification system among two mobile nodes in MANET, hence it becomes almost impossible task to identify the nodes to be regular or malicious.

A malicious node can easily furnish false information at the time of route discovery process by other regular nodes; they choose to participate even in node forwarding in the preliminary phases. This treacherous act of malicious mobile node will eventually gain the trust and belief system of the network where the malicious nodes seek for an optimal opportunity to initiate a brutal attack on the network. It is to be noted that once the malicious node gains the trust, the more is the intensity of the attack potentially damaging various resources in MANET system. One of the most critical issues of such phenomenon is the identification of behavior of different types of nodes. In (Khan et al., 2013) authors have elucidated the malicious behavior of node in detail along with assessment of different security mechanisms in place to mitigate the same.

III. STUDY ON MALICIOUS/SELFISH BEHAVIOUR

This section discusses about the set of literatures that has been introduced in the past for the purpose of mitigating the malicious or selfish behaviour of a mobile node in MANET.

The early prominent work in this direction has been discussed by (Schutte, 2006) who has outlined some of the critical and potential threats in mobile adhoc network and recapitulated popular approaches to develop secure MANET protocols in order to identify selfish nodes and to enforce cooperation. The author also brings forth the concept of Erroneous nodes in MANET environment and clarifies some of the misconceptions in the understating of selfishness and misbehavior of nodes.

A critical analysis of the previous research in the direction of misbehavior problem of nodes and its impact on the overall performance of a MANET has been presented in (Rizvi and Elleithy, 2009). Furthermore, the authors have also proposed a mathematical model based on the time division technique to minimize the misbehavior of mobile nodes while avoiding unnecessary elimination of these nodes unlike CONFIDANT (Buchegger and Le, 2002) and CORE (Michiardi and Molva, 2002). The presented approach not only improves the resource sharing but also creates a consistent trust and cooperation (CTC) environment among the mobile nodes. The simulation results obtained demonstrate the success of the proposed approach in terms of significant reduction of the misbehavior being exhibited by nodes and consequently maximizing the overall throughput of MANET than other well-known schemes. However while addressing the problem of misbehavior of nodes the authors have modeled the malicious and selfish nodes in the same manner without considering any further sophistication on the part of malicious nodes in conducting attacks or modeling the utility functions of the two separately. The developed model actually can be seen as to mitigate selfishness not malicious behaviour.

A secure route discovery mechanism for MANETs using Ad-hoc On-demand Distance Vector (AODV) routing protocol against two of the most common Denial-of-Service (DoS) attacks, Blackhole attack and Grayhole attack that disrupt route discovery process by sending forged routing information was illustrated in (Jhaveri et al., 2012). In this technique, a mobile node identifies abnormal routing information when it receives route reply from misbehaving neighbor mobile node launching attack and alerts other mobile nodes about the opponent without using additional control packets; routing packets are used not only to pass routing information, but also to broadcast information about malicious mobile nodes. The solution isolates multiple malicious mobile nodes during route discovery procedure and assures selection of short and secure route to destination. Simulation results in ns-2 prove the consistency and efficiency of the protocol.

Efficient framework to detect malicious behaviour of nodes so that a route via malicious node is never used to transmit an application packet to its destination has been put forth by (Gupta and Mehrotra, 2013). When a data packet destined for some other node reaches a malicious node because of the route it was supposed to take, rather than forwarding the same to the appropriate node the malicious node simply drops the packet. The problem is adverse when malicious nodes exist in comparable numbers within the network. Inproposed work, the authors overcome this problem by identifying such maliciousbehaviour of nodes and then a route via such a node is never chosen by its neighbor to forward an application packet in the network. The model developed by the authors is not applicable to other routing protocols else than AODV. The major shortcoming of the paper is that there has not been any line drawn between the malicious and selfish behaviour of nodes. The work is also based on the assumption that there are no selfish nodes existing within a MANET environment, otherwise the system will lead to false reporting and later network partitioning may occur. Again the authors have modeled the malicious nodes as weak, not considering they may change their strategies as per requirements.

A novel technique for tracing the malicious nodes in mobile adhoc network (MANET) has been introduced by (Karjee and Banerjee, 2008). As the mobile hosts are free to move anywhere and can change the wireless topology frequently, each node within a MANET are much more vulnerable to insider attacks specially under noise and external attacks due to lack of permanent infrastructure, limited resources, absence of central administrator, etc. The authors have done an investigation and mathematical analysis based upon the detection of malicious node with attack modeling .The authors have proposed a scanning procedure and security measures for the multi hop wireless network after diagnosing the abnormal behavior of malicious node and verifyingthe physical presence of attack strategy in wireless network. The model has not been validated for major routing issues like interference, asymmetric links channel capacity and effects of noise, etc. have not been taken into account. Furthermore, the work seems to be done on the assumption that selfish nodes never exist in MANET system.

An efficient project of Selfish node detection method with novel replica allocation techniquesto handle the selfish replica allocation property has been done by (Suganya and Priya, 2013). In the discussed method, each node computes credit risk information on other associated nodes individually to appraise the degree of selfishness. The Routing misbehavior mitigation decreases the overall recognition time with a condensed cost in term of message overhead. This decline is very important when the watchdog detection effectiveness is low down. In addition, this diminution can be attained even with a reasonable extent of collaboration. Widespread simulation results illustrate that the projected strategies outperform existing representative supportive replica allocation methods in terms of data accessibility, communication cost and query delay. However, there does not exist any updating strategy to take into account the effect of false positives or false negatives in the model. Again there is no mentioning of malicious nodes which can take advantage of the presence of selfish nodes in the network. The model developed by the authors does not take into account the malicious nodes can also exist within the network along with selfish nodes.

The topic of Selfish Nodes within a Mobile Ad-Hoc Networks (MANET), specifically sensor networks due to their lower power and bandwidth has been discussed by (Probus, 2007). The approach used is a reputation based algorithm to isolate the selfish nodes from communication by using past history to determine how reliable the node is. By using the proposed algorithm within Destination-Sequenced Distance Vector routing protocol (DSDV), functionality and performance has been shown to be increased in the Wireless Sensor Networks. As a result of the isolation, retransmission is decreased and throughput increased, therefore conserving power consumption of individual nodes and creating a more reliable network by having less error rate and spare bandwidth. The proposed algorithm overlooks the possibility for existence of malicious nodes in the network. However it would be worth mentioning here the problem of malicious nodes or intrusion is not associated with sensor networks in the same dimension unlike the traditional MANET system.

A concrete investigation on the security mechanisms that are proposed for Selfish node attack in MANETs with the aid of a well-known multicast routing protocol namely Multicast Ad hoc On Demand Distance Vector (MAODV) has been done by (Sengathir and Manoharan, 2013). The authors propose an algorithm called Secure Destined Packet Algorithm as an add-on to secure the MAODV protocol against non-cooperating nodes.The proposed security solutions is evaluated in terms of three parameters namely packet delivery ratio, control overhead and total overhead. The algorithmic solution is analyzed in the simulation environment by using ns-2 simulator. The evaluation shows that enhancement in the efficiency of the MAODV protocol when selfish nodes exist in comparable numbers within the MANET system. However, there is no boundary drawn between selfishness and malicious behaviour in this work. Again the misbehaving nodes have been modeled as fragile which don’t change attacking strategies to evade detection.

The simulation study of the security algorithm that detects misbehaving links in Mobile Ad Hoc Networks has been studied by (Kumar et al., 2011). The system implements the 2ACK scheme which helps detect misbehavior by a 2 hop acknowledgement. The 2ACK scheme for detecting routing misbehavior is considered to be network-layer technique for mitigating the routing effects. The 2ACK scheme identifies misbehavior in routing by using a new acknowledgment packet, called 2ACK packet. A 2ACK packet is assigned a fixed route of two hops (three nodes N1, N2, N3), in the opposite direction of the data traffic route. The simulations conducted show that more than 90% packet delivery ratio even with 40% misbehaving nodes existing in the MANET system while the usual Dynamic Source Routing Protocol (DSR) scheme maintain a packet delivery ratio of only 40%. However authors have concentrated only on the Link misbehavior rather than the node misbehavior although the same could have been established by scrutinizing of all the links that the particular node is part of. Also the results are only got with a single routing protocol and it is also not clearly mentioned whether the proposed scheme works on the top of other routing protocols. Further the system has modeled the selfish and malicious nodes together as misbehaving nodes. The summary of the above recent work is tabulated below:

Table 1.Summary of the findings

Author	Contribution	Result Obtained	Limitations
(Rizvi and Elleithy, 2009).	-Critical analysis of the previous research work. -Presented analytical model to mitigate node misbehavior.	-With Elimination of nodes occurring frequently the performance of the adhoc network falls substantially. -Better performance as compared to CONFIDANT (Buchegger and Le, 2002) and CORE (Michiardi and Molva, 2002) in terms of throughput and transmission overhead.	-Misbehaving nodes modeled as weak. -No difference between selfish and malicious nodes while modeling the utility functions of the two.
(Suganya and Priya, 2013).	New replication allocation technique	Reduced routing misbehavior in delay tolerant network.	-Effect of false positives is not considered. -Existence of Malicious Nodes not considered.
(Probus,2007).	Reputation based technique to separate selfish nodes.	-Increased throughput. -Conservation of channel capacity -Effective network creation.	Not applicable to other routing protocols except DSDV.

(Sengathir and Manoharan, 2013).	Developed a security add-on for Multicast Adhoc On Demand Distance Vector protocol.	Effective in detecting misbehaving node.	-No line drawn between Selfish and Malicious Nodes. - Malicious Nodes Modeled as fragile. - Not applicable to other routing protocols.
(Kumar et al., 2011).	Designed a novel mechanism to detect misbehavior by a 2 hop acknowledgement.	-Increase in Packet delivery ratio with the add-on for the DSR routing Scheme. - System works pretty good even in presence of comparable number of misbehaving nodes.	-Focused on the problem of detecting misbehaving links instead of misbehaving nodes. -Result fetched on a single Routing Protocol i.e. DSR -Effective only with a dense MANET environment.
(Karjee and Banerjee, 2008).	A novel technique for tracing the malicious nodes in mobile adhoc network based on noise errors in different frequency bandwidths.	Diagnosis of the abnormal behavior of malicious nodes	- Not validated for major routing issues like interference, asymmetric links channel capacity, etc. - Effects of noise not considered. -Selfish nodes never exist in MANET system.

IV. WORK USING GAME THEORETIC APPROACH

While reviewing some more techniques on security system in MANET, it was also found that game theory has also prime contribution in past few years due to potential accuracy in its probabilistic approach and computational efficiency. This section discusses about the various works that has been witnessed in the literaturewhich have taken help of Game Theory in the process of securing MANETs.

A model constructed upon mechanism design allowing clusters with single trusted node acting as certificate authority (CA) to be formed has been proposed by (Rachedi et al., 2010). The prime aim of the proposed system is to stimulate non-confident community nodes for participation by allocating to them trust based incentives for the same. These trust incentives can later be used by the same nodes to avail different cluster services. The results show the security of the CA is being preserved, which leads to prolongation of the cluster lifetime. Again the model is able to shrink the size of the cluster which hints to increase in the number of clusters being formed. This leads to network stability and efficiency in serving the cluster nodes. However, neither malicious behavior on the part of cluster nodes is considered nor any sort of security validation of the proposed model has been done.

The problem of intrusion in MANETs and a few totally different solutions of this downside supporting the approach of theory of games have been analyzed by (Javidi and Aliahmadipour, 2011). The authors have evaluated four approaches based on Game Theory that claim to improve the performance of the Intrusion Detection System using: Clustering, Number of Nodes having IDS capability, Competence for detecting misbehaving selfish nodes and Energy efficiencies of the schemes as the performance metrics. The advantages and disadvantages associated are also mentioned clearly.

A novel credit-based cooperation mechanism that utilizes hash chains on messages to defend against cheating by the nodes has been presented by (Janzadeh et al., 2009). The author showed that it imposes a low workload on the nodes in comparison with the mechanisms that deploy digital signature schemes. Moreover, through a game-theoretic analysis, it is shown that any level of cooperation by a node will be attainable if the mechanism makes appropriate payments. However the scalability of the approach is not discussed and there also exists scope for enhancement to the strategies employed, the coordination between malicious nodes is not considered, and the malicious nodes are modeled as fragile. Furthermore the hash chains are vulnerable to rainbow attacks.

A Game theory based security add-on called as (AODV-GT) for the reactive AODV (Adhoc On-Demand Distance Vector) routing protocol has been proposed by (Panaousis and Politis, 2009). The add-on is aimed to provide guard against the black hole attack in MANETs. The same is based on the concept of non-cooperative non-zero games and when integrated with AODVthe packet drop ratio decreases immensely as compared to when employing AODV unaided, in the existence of black hole nodes within the MANET environment. The simulations are conducted using the network simulator ns-2. However it is being assumed by the authors that HIDS sensors exist in the network and they are responsible for detection and elimination of the malicious nodes, thus malicious behaviour is left untouched. Again, the add-on developed is not applicable to other routing attacks and neither can work on the top of other MANET routing protocols.

A repeated-game forwarding model based on the global punishment mechanism to enforce cooperation among nodes and to mitigate selfish behaviour has been proposed by (Wang and Wu, 2012). The authors also emphasize upon the conditions which lead to reaching of Nash Equilibrium for the cooperative state of the MANET system. The strength is of the model unlike many of the previous works the model takes rationality of misbehaving nodes, which is selfish nodes in this case, into consideration. Selfish nodes are not modeled as fragile. Simulation conducted proves that the proposed model is able to enforce cooperation among the selfish nodes. However there is no effort being done over malicious behaviour mitigation or analyzation. The model is not applicable with Sybil attack, newcomer attack, bad-mouthing attack, etc.

(Li et al., 2013) proposed a game theoretic framework to analyze the strategy profiles for regular and malicious nodes. The work done by the authors is highly empirical and all nodes from opposite sides are modeled to be completely rational regarding concern with playing the game with each other. The wrestling between the regular and malicious nodes has been modeled as Multistage Bayesian Signaling Game. However the authors undermine the fact that some regular nodes may start behaving selfishly in the due course of the game.. The rationality of nodes is node is not taken care of while designing the decision making model of the regular malicious node game with the intention of discouraging selfish behavior on the part of regular nodes.

. Table 2 Summary of the findings

Author	Technique Used	Result Obtained	Limitations
(Rachedi et al., 2010).	Applied Reverse game theory on cluster model to simulate cooperation.	-Prolonged cluster lifetime. - Increased number of clusters and reduction inCluster's size.	-Validation with respect to security is not done. -Malicious behaviour is not discussed
(Panaousis and Politis, 2009).	Game theory based security add-on called as (AODV-GT) for the AODV to guard against black hole.	Packet drop ratio decreases immensely as compared to when employing AODV alone.	-Not applicable for other routing attacks. -Malicious behaviour is not studied.

(Wang and Wu, 2012).	Global punishment based repeated-game model to stimulate node cooperation.	-Proposed model enhances node forwarding probability	-Focusing on the node forwarding process rather than malicious behaviour detection or analysis. -Not applicable for Sybil attack, newcomer attack, collusion attacks.
(Li et al., 2010)	Proposes a game theoretic framework to analyze the strategy profiles for mobile nodes.	Proposed PBE strategy outperforms both pure and mixed strategies.	-Does not consider the selfish nodes in the regular node camp. -Collusion between Malicious nodes not taken.

V. OPEN ISSUES

Although there are various numbers of issues pertaining to various problem domains in MANET, but in order to narrow down the focus of exploring open issues, paper considers the following are the critical open issues after reviewing the literatures in the previous section:

- The incorporated properties of the MANET system are the sole reason for quality of services too. Although all works like (Karjee and Banerjee, 2008), (Rizvi and Elleithy, 2009), (Sengathir and Manoharan, 2013), (Panaousis, 2009), etc. that addresses the routing security, at the same time fail to address specifically other critical issues like channel capacity (packet delivery ratio, bandwidth, jitter, delay etc.). It can be seen from all these above mentioned work that although the optimal security is established, but it has no positive effect on QoS parameters.
- There are exist a quite a large no of attacks in MANETs like Rushing attack, Wormhole Attack, etc. which require coordination and collusion among the attacker nodes. None of these sophisticated attacks have been actually modeled using Game Theory although there is a scope for the same.
- In MANET environment, the presence of selfish node is potentially harmful as the similar behavior of the selfish node can be easily imitated by malicious node. None of the above previous works which have either tried to model the behaviour of malicious node or to mitigate the effects of the same, while considering the presence of selfish nodes along with normal collaborating nodes in the Regular Champ. The two have not been differentiated while addressing one of them.
- A malicious node may exhibit an abnormal behaviour even in its mobility also, which has not been considered in any test bed of the security techniques discussed found so far.

VI. CONCLUSION

The paper has probed into some of the current research work that claims to address the issues relating to malicious / selfish behaviour of nodes in MANETs. The outcome of the study is that although there are quite few researches works that have been carried out to counter the problem of node misbehavior, but there still exist the wide range of open issues that need to be taken for mitigating the same completely especially the concurrent consideration of selfish and malicious nodes in the network while designing a extenuation technique.

REFERENCES

Belding, E.M., Al-Agha, K., Pujolle, G. (2004). Mobile and Wireless Communications Networks, Springer

Buchegger, S., & Le Boudec, J. Y. (2002, June). Performance analysis of the CONFIDANT protocol. In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing (pp. 226-236). ACM.

Gupta, A. K., &Mehrotra, D., (2013). Detecting and Dealing with Malicious Nodes Problem in MANET. In International Journal of Scientific & Engineering Research, 4(7), 161-166

Janzadeh, H., Fayazbakhsh, K., Dehghan, M., &Fallah, M. S. (2009).A secure credit-based cooperation stimulating mechanism for MANETs using hash chains. Future Generation Computer Systems, 25(8), 926-934.

Javidi, M. M., &Aliahmadipour, L. (2011). Game theory approaches for improving intrusion detection in MANETs. Scientific Research and Essays, 6(31), 6535-6539.

Jhaveri, R. H., Patel, S. J., Jinwala, D. C., Ferreira, E. A., de Mello, R. F., Yu, L., ... & Silva, P. S. M. (2012). Improving route discovery for aodv to prevent blackhole and grayhole attacks in manets. INFOCOMP Journal of Computer Science, 11(1), 1-12.

Karjee, J., & Banerjee, S. (2008, October). Tracing the abnormal behavior of malicious nodes in MANET. In Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on (pp. 1-7). IEEE.

Khan, B. U. I., Olanrewaju, R. F., & Habaebi, M. H. (2013). Malicious Behaviour of Node and its Significant Security Techniques in MANET-A. Australian Journal of Basic and Applied Sciences, 7(12), 286-293.

Kumar, A., Kadam, V., Kumar, S., &Pawar, S. (2011). “An Acknowledgement

Based Approach for the Detection of Routing Misbehavior in MANETS. International Journal of advances in Embedded Systems, 1(1).

Li, F., Yang, Y., & Wu, J. (2010). Attack and flee: game-theory-based analysis on interactions among nodes in MANETs. Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on, 40(3), 612-622

Makki, S.K., Reiher, P., Makki, K., Pissinou, N., Makki, S. (2007). Mobile and Wireless Network Security and Privacy, Springer

Michiardi, P., & Molva, R. (2002). Core: a collaborative reputation mechanism to

enforce node cooperation in mobile ad hoc networks. In Advanced Communications and Multimedia Security (pp. 107-121). Springer US.

Panaousis, E. A., &Politis, C. (2009, October). A game theoretic approach for securing AODV in emergency Mobile Ad Hoc Networks. In Local Computer Networks, 2009. LCN 2009. IEEE 34th Conference on (pp. 985-992). IEEE.

Probus, M. W. (2007). Selfish node isolation in mobile ad-hoc networks (Doctoral dissertation, University of Louisville).

Rachedi, A., Benslimane, A., Otrok, H., Mohammed, N., & Debbabi, M. (2010).A Secure mechanism design-based and game theoretical model for MANETs. Mobile Networks and Applications, 15(2), 191-204.

Rizvi, S. S., & Elleithy, K. M. (2009).A New Scheme for Minimizing Malicious Behavior of Mobile Nodes in Mobile Ad Hoc Networks.arXiv preprint arXiv:0908.0981

Schutte, M. (2006). Detecting Selfish and Malicious Nodes in MANETs. HPI/UNIVERSITÄT POTSDAM, SOMMER SEMESTER.

Sengathir, J., &Manoharan, R. (2013).Security Algorithms for Mitigating Selfish and Shared Root Node Attacks in MANETs.International Journal of Computer Network and Information Security (IJCNIS), 5(10), 1

Suganya, N. R., &Priya, S. M. (2013). Detecting Selfish Nodes in a MANET through Fragmentation in Distributed Environment. International Journal of Science, Engineering and Technology Research, 2(6), pp-1370.

Wang, K., & Wu, M. (2012). Nash Equilibrium of Node Cooperation Based on Metamodel for MANETs. Journal of Information Science and Engineering, 28(2), 317-333

Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004). Security in mobile ad hoc networks: challenges and solutions. Wireless Communications, IEEE, 11(1), 38-47.