A Cooperative Black hole Avoidance Scheme of Intrusion Detection System in Mobile Ad Hoc Networks

V. Rajanesh

Assistant Professor, Department of ECE, JNTUH College of Engineering Sultanpur, Telangana, India.

Abstract— The Mobile Ad hoc Networks (MANET) remain self-configuring, infrastructure less, dynamic wireless networks wherein the nodes serve as the restricted resources. The implementation of the Intrusion Detection Systems (IDS) is done within the MANETs for monitoring the operations for detecting some of the intrusion within the additional vulnerable network. This paper presents the effective methods to analyse as well as optimise the time duration where the intrusion detection schemes must be active within a MANET. Therefore, it is quite challenging to prevent or to detect the mischievous nodes that launches the grayhole or collaborative blackhole attacks. The challenges in the designs of the dynamic source routing (DSR)-based routing methods that is considered as the cooperative black hole avoidance scheme (CBAS) where the benefits of the either proactive as well as reactive defense architectures are integrated are resolved by this paper. The existence of the malicious-node attacks can be shown in the Simulation results and the EAACK & PM-IDs with respect to End to End delay, energy consumption, as well as throughput are outperformed by CBAS.

Index Terms—Ad hoc networks, intrusion detection, energy efficiency, CBAS, black hole attacks, MANET.

I. INTRODUCTION

A self-organized mobile nodes collection that communicates with one another exclusive to the assistance of a fixed infrastructure or the central coordinator is referred as MANET. Node is referred as a mobile device which is having the capability of communicating with the additional devices. The role of the host and the router is played by the node within MANET. The assistance is taken by the intermediate nodes by the nodes for relying the individual messages for communicating with the additional nodes which are not in their communication range. The variation in the network topology occurs with respect to time with the movement of the nodes and certain nodes are joined within the network where some of them are disengaged out of the respective networks. Various benefits are possessed by MANETs compared to the conventional schemes wherein the setting up or dismantling in addition to the supply of the flexibility where the tethering of the nodes is undone.

The attachments of the ad hoc networks can be done with the internet or the additional networks except that are operative by means of a stand-alone network and therefore, it is quite significant to extent the connection as well as coverage for the regions in which the fixed infrastructures are not present. Various regions are covered by the existing and future applications of MANET. Vehicular ad hoc network (VANET) is classified among the significant application scenario. A self-configuring network of the moving vehicles even though the moving pattern of the nodes are constrained by the road course, traffic regulations and so on is referred as VANET. Moreover, it refers to an optimistic approach which is having an enormous possibility for improving the safety of the vehicle as well as road traffic effectiveness in addition to convenience ([1]-[2]).

It is quite complex to provide safety in MANET because of the innate features of MANET like mobility, wireless communication links as well as the lack of some of the centralized authority. In addition, the adaptation of the security solutions on behalf of the fixed wired networks towards mobile wireless networks is not easy. Intrusion detection is a technique that monitors the operation within the system for determining if there exists any violation of the safety requirements and moreover it is used to provide safety for MANET. An approach implemented by the network nodes to detect the intrusion is referred as Intrusion Detection System (IDS) and it is divided within 2 classes depending upon the methods used i.e., (a) Signature-based intrusion detection and (b) Anomaly-based intrusion detection.

The incorporation of the data regarding the signatures of attacks is done within the detection system in signature-based detection approach. The features of the attacks are similar to the signature incorporated within the IDS by the occurrence of an attack. The attack corresponding with the signature occurs when the above mentioned are matched. Finding the match for the signature is not attempted by IDS within the anomaly-based detection and however it searches for the anomalous events or performance. For example, the anomalous behavior are paying attention towards the abnormal performance including the data packet dropping as well as the events that includes the irregular variations within the routing table. The classification of IDSs are done depending upon the audit information utilized for analysing.

The information gained out of the host where the intrusion detection is verified and is implemented within the Host-based IDSs. The data can serve as the operating network or the application is logging upon this network. However, the data coming out of the network traffic is collected as well as analysed by the network-based IDSs. The network-based anomaly detection mechanism is focused in this paper.

Although extensive efforts are done to design the efficient IDSs, less efforts were done upon the effective implementation of IDSs. It plays a crucial role within the resource-controlled condition. Addressing the issues in this paper is attempted severely. The detection system is resting upon each node that is operated continuously within the existing IDSs for MANETs. Traffic monitoring within the range of the nodes is a technique implemented by these IDSs ([3]-[8]). It is quite expensive for operating IDSs continually due to the computational resources. Therefore, reducing the duration for an IDS that must be active exclusive to the compromise of the efficiency is a challenging task. The abovementioned challenges might be not be significant due to the deployment of IDS within the stationary route or gateway by the help of the virtually unlimited computational as well as the battery power. A crucial role is played with respect to MANETs in which the role of hosts or routers is played by the individual mobile nodes and moreover, the operations like intrusion detection which may be collaboratively or individually must be performed by them. In this regard, a distributed method is proposed on behalf of the effective utilization of IDSs within a network depending upon the probability concept.

The circumstances wherein the players are coordinating the individual strategy as well as distribute the payoffs among them are modelled by this Cooperative game theory. In order to break away the incentive of none of the players out of coalition, the game out should be balancing ([30]-[32]).

Two opposing sets of players i.e., the nodes/IDSs as well as attacker/defaulters are involved by the settings of the game within the entire earlier game-theoretic operations upon IDS. A game in which the players who cooperate in achieving a common goal is involved in this paper. This paper discovered various operations upon the cooperation of the IDSs where such circumstances are modelled with the help of the game theory. The communication among the IDSs within the region are modelled by the presentation of these kind of cooperative multi-player game and moreover the presented probabilistic approach is validated by using this.

II. RELATED WORK

The existing related work upon the energy efficient usage of intrusion detection systems in a MANET is presented in this section. A proper investigation upon the optimization of the network topology on behalf of controlling the edge-self within the sensor networks by the intention to maximize the network lifetime is provided in [9]. The number of the monitoring nodes are reduced by optimizing the selection of the monitoring of the nodes which controls the communications links. Although the conservation of energy is the main intention, this paper concentrates upon the reduction of the active duration of the monitoring nodes despite the reduction of the monitoring nodes. Minimisation of the monitoring nodes which in turn monitors the communications is focused in the existing method. Therefore, the overall load in controlling the communications links during the sleeping condition of the sleep nodes is endured by the active nodes. Although the consumption of energy is minimized completely, certain energy within few nodes might get reduced quickly compared to the other nodes. Each neighbour contributes within for sharing the profit amid every nodes is performed despite the placement of burden in controlling upon some of the nodes.

In order to monitor the sensor networks, the specific nodes named as *guard* nodes are used by the protocol SLAM [10]. In general, the guard nodes exists within the sleep mode. The guard nodes which is in charge of local monitoring upon the respective next hop is awakened by the nodes earlier to the communication upon a link. Reducing the duration taken by the guard node for awakening the nodes that monitors the mischievous activities is the major objective of this method. It is discovered that a connection amid the nodes is present when monitoring the network. The probability wherewith the individual IDS is monitoring as well as scheduling the monitoring period despite of the additional nodes is determined in this paper. In addition, most of the overall guard nodes within SLAM maybe awake during the application of several communication links that moreover refers to a drawback.

A technique on behalf of the optimum selection as well as the energizing of the intrusion detecting agents on behalf of WSNs is proposed in [11]. The intrusion agents can be activated by the nodes that are having the trust value higher than the necessity for monitoring the packets as well as for sending the alerting packets to the cluster heads. Therefore, it is necessary for every single node for maintaining an insignificant trust database of the individual neighbours in addition of the clustering of the nodes. The obtained safety level in [12] is guaranteed by a game theoretic technique on behalf of the distributed intrusion detection schemes within the ad hoc networks where the network lifetime is maximised. An assumption is made by the authors that the division of the network is done within the clusters of nodes wherein certain nodes are trusted. A perfect IDS is used to equip a trusted nodes in order to performed the intrusion detection and it is efficient on behalf of the overall cluster that any additional nodes is not included within the process of monitoring. As compared, no node is assumed as perfect in this paper. The simulation results presents the presence of the energy efficiency trade-off as presented in [12]. Above all, the network is assumed as static by the previous works ([9]-[12]) whereas some of the nodes are mobile. A method [13] wherein the selection of the subset of nodes within a dynamic network is proposed where a subset of nodes is monitored by every single node in order to reduce the monitoring traffic or to select the prediction of the nodes that are assumed to be long-living. The overall data collected within a multi-channel wireless network is reduced [14] in the optimum selection of m from M sniffers as well as the allotment of every sniffer for a single K channel. Nevertheless, the similar objective is not shared by this paper.

The context of wired networks ([15]-[16]) studied the minimization of the consumption of energy using the intrusion detection systems. The energy-latency trade-off is resolved by the presentation of an architecture (LEoNIDS) on behalf of the network-level intrusion detection system with the supply of low power consumption as well as the detection latency simultaneously in [15]. The consumption of energy is reduced while detecting the intrusion on behalf of the networking security control systems by using the Packet-based selective encryption in [16].

The intrusion detection within the wireless networks [17]-[24] is modelled by using the Game theory. The literature presents various additional game-theoretic solutions which monitors the problems such as cooperation as well as node selfishness within the network [25]-[29].

III. PROPOSED SYSTEM

This paper presents a method in which the mischievous nodes are detected efficiently and which are attempting for launching the grayhole/collaborative blackhole attacks. The mischievous nodes for sending a reply RREP message are baited in this method by using the address of adjacent nodes and a reverse tracing approach is used to detect the mischievous nodes. In order to alert the overall nodes for stopping the communication by the additional nodes within the list, a detected mischievous nodes is placed within the blackhole list. The advantage of CBAS is that the proactive as well as the reactive defence architecture for achieving the abovementioned objective is integrated compared to the existing methods.

A neighbouring node for incorporating is selected by the source nodes in this technique. Moreover for addressing the node, the implementation of nodes is done as bait destination addressing for baiting the mischievous nodes for sending a reply RREP message. The participation of the mischievous nodes within the routing are avoided as well as recognised with the help of a reverse tracing approach. An assumption is made in this context that during the essential dropping within a packet delivery ratio, the destination node sends an alarm to the source node for triggering the detection technique. The benefits of the proactive detection within the early stage as well as the advantage of the reactive response at the subsequent stages for reducing the wastage of the resources are merged by CBAS scheme.

3.2 The CBAS mechanism working as three main steps:

1) Initial setup
2) Initial reverse tracing step
3) Shifted to reactive defense step

3.2.1 Initial setup:

By the sending of bait RREQ which was implemented for advertising as possessing the shorter path towards the nodes which is detaining the converted packets, a mischievous node must send a reply RREP message for achieving the destination address of the bait RREQ.

3.2.2 Reverse tracing technique:

The performance of the mischievous nodes across the route reply towards the RREQ message can be detected by using this. A false RREP is sent by a mischievous nodes when a RREQ is received. Therefore, the similar procedure is continued on behalf of the overall nodes as well as the RREP is received for reducing the data regarding the doubtful path in addition to the temporarily trusted zone within the route.

The time duration of the packet delivery is fixed with the help of dynamic threshold algorithm and the various time intervals depending upon the performance of the node is compared by the node threshold. The node threshold which is below 0.95 is later increased to 0.01 or when it is above 0.95, it is later decreased to 0.01. The working of the reverse tracing technique is shown in the following figure. In the following figure, n1 serves as source node and n6 acts as a hop neighbor node.

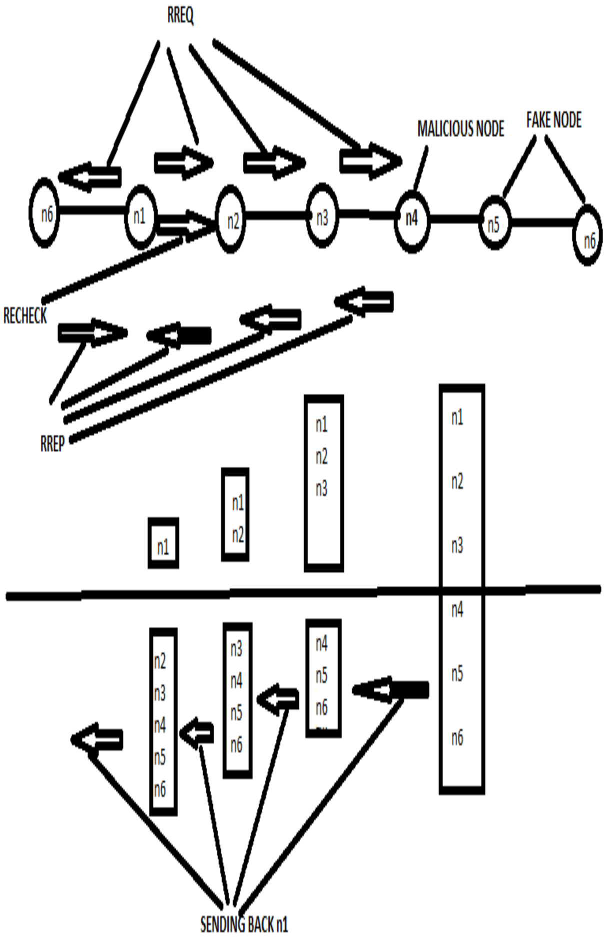

Figure 1: Reverse Tracing Technique

3.2.3 Shifted to reactive defense phase:

After the establishment of a route, when it is discovered that the packet delivery ratio is dropped down to threshold, then the triggering of the detection technique is done for detecting the constant maintenance as well as the real-time reaction efficiency. The designing of a dynamic threshold is done in this paper wherein the time during the falling of the packet delivery ratio in similar threshold is controlled.

IV. RESULTS AND DISCUSSION

The transmission of the data is done in packets that has a 512 bytes size having CBR as application traffic by 10 packets/sec transmission rate. 28 m/sec of maximum speed is used and 15 MBPS of data rate is used in the channel. The region of 1216x743 is used by the overall network and 18 nodes are implemented where, the role of mischievous nodes is played by nodes 1,2,3,4. This paper considers the threshold value and 50 sec of total simulation is assumed.

PARAMETER	VALUE
Application traffic	CBR
Transmission rate	10 packets/sec
Radio range	250m
Packet size	512 bytes
Simulation time	50secs
Number of nodes	18
Area	1216x743
Malicious nodes	1,2,3,4
Threshold	Dynamic threshold
Routing Methods	EAACK, PM-IDS, CBAS

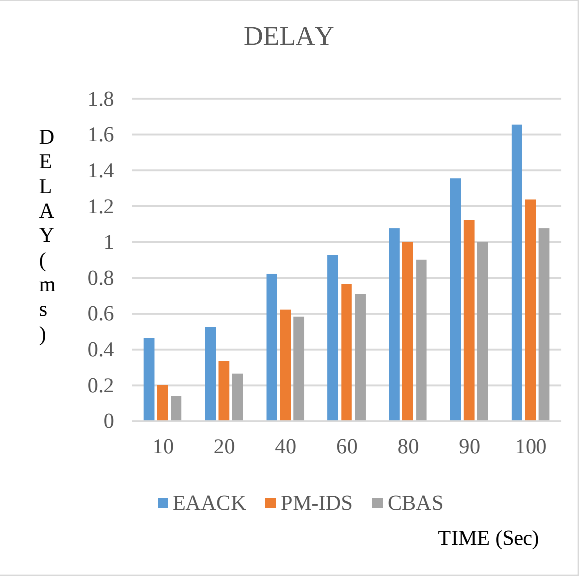

Figure 2: End-to-End Delay

The End-to-End Delay of the network is shown in the above Figure 2. The reduced delay must be considered in this method compared to the existing PM-IDS, EAACK approaches for obtaining the improved network performance.

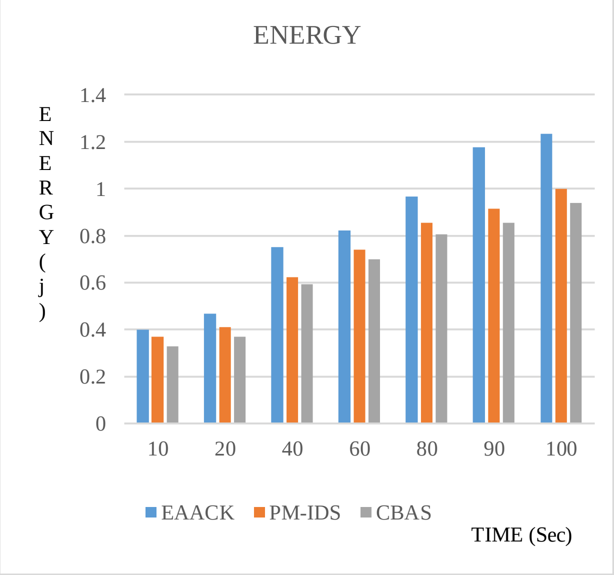

Figure 3: Energy Consumption

The Energy Consumption of the network is shown in Figure 3. Lower Energy Consumption is considered in this CBAS approach than the PM-IDS, EAACK approaches for obtaining the improved network performance.

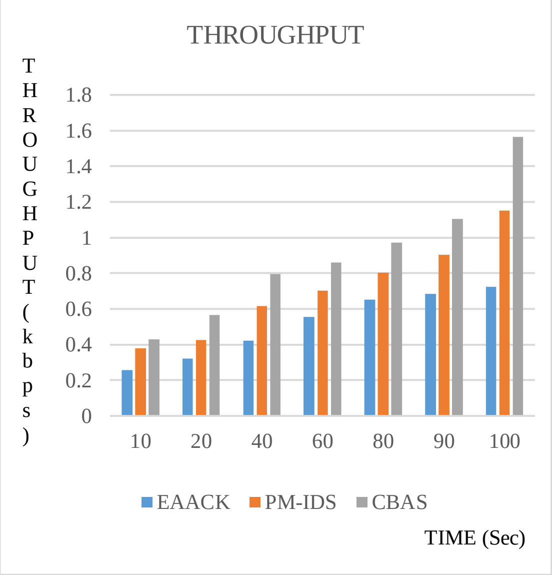

Figure 4: Throughput

The network Throughput is shown in Figure 4. Higher throughput is considered in this CBAS system than the previous techniques such as PM-IDS, EAACK for obtaining the enhanced network performance.

V. CONCLUSION

This paper proposes a novel technique named as CBAS to detect the malicious nodes within MANETs using the collaborative or gray blackhole attacks. It is shown in the simulation outcomes that the DSR, 2ACK, and BFTR techniques are outperformed by CBAS with respect to packet delivery ratio as well as routing overhead. It is intended for 1) investigating the feasibility to adjust CBAS for addressing the additional kinds of the collaborative attacks upon MANETs as well as for 2) investigation the incorporation of CBAS using famous message security approaches for constructing an extensive secure routing technique for protecting the MANETs from the miscreants for the future work.

VI. REFERENCES

[1] S. Zeadally , R. Hunt, Y-S. Chen, A. Irwin and A. Hassan, ”Vehicular ad hoc networks (VANETS): status, results, and challenges,” Telecommunication Systems, vol. 50, no. 4, pp. 217-241, 2012.

[2] S. K. Bhoi and P. M. Khilar, ”Vehicular communication: a survey”, IET Networks, vol. 3, no. 3, pp. 204 - 217, 2014.

[3] S. Marti, T. J. Giuli, K. La and M. Baker, ”Mitigating Routing Misbehavior in a Mobile Ad-hoc Environment,” Proc. 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 255-265, August 2000.

[4] C. Manikopoulos and L. Ling, ”Architecture of the Mobile Ad-hoc Network Security (MANS) System,” Proc. IEEE International Conference on Systems, Man and Cybernetics, vol. 4, pp. 3122- 3127, October 2003.

[5] K. Nadkarni and A. Mishra, ”Intrusion Detection in MANETs – The Second Wall of Defense,” Proc. IEEE Industrial Electronics Society Conference ’2003, pp. 1235-1239, Roanoke, Virginia, USA, Nov. 2-6, 2003.

[6] A. Partwardan, J. Parker, A. Joshi, M. Iorga and T. Karygiannis, ”Secure Routing and Intrusion Detection in Ad-hoc Networks,” Proc. 3rd IEEE International Conference on Pervasive Computing and Communications, Hawaii Island, Hawaii, March 8-12, 2005.

[7] N. Marchang and R. Datta, ”Lightweight Trust-based Routing Protocol for Mobile Ad Hoc Networks,” IET Information Security, vol. 6, no. 4, pp. 77-83, 2012.

[8] N. Marchang and R. Datta, ”Collaborative Techniques for Intrusion Detection in Mobile Ad-hoc Networks,” Elsevier Ad Hoc Networks, vol. 6, no. 4, pp. 508-523, June 2008.

[9] D. Dong, X. Liao, Y. Liu, C. Shen and X. Wang, ”Edge Self-Monitoring for Wireless Sensor Networks,” IEEE Transactions on Parallel and Distributed Systems,” vol. 22, no. 3, March 2011, pp. 514-527.

[10] I. Khalil, S. Bagchi and N. B. Shroff, ”SLAM: Sleep-Wake Aware Local Monitoring in Sensor Networks,” Proc. 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2007 (DSN 2007), 565-574.

[11] T. Hoang Hai and E-N. Huh, ”Optimal Selection and Activation of Intrusion Detection Agents for Wireless Sensor Networks,” Proc. Future Generation Communication and Networking (FGCN 2007), vol.1, no., pp.350-355, 6-8 Dec. 2007.

[12] S. M. Fitaci, K. Jaffres-Runser and C. Comaniciu, ”On modeling energysecurity trade-offs for distributed monitoring in wireless ad hoc networks,” Proc. Military Communications Conference, 2008. MILCOM 2008. IEEE , vol., no., pp.1-7, 16-19 Nov. 2008.

[13] R. G. Clegg, S. Clayman, G. Pavlou, L. Mamatas and A. Galis, ”On the Selection of Management/Monitoring Nodes in Highly Dynamic Networks,” IEEE Transactions on Computers, vol.62, no.6, pp.1207-1220, June 2013.

[14] R. Zheng, T. Le and Z. Han, ”Approximate Online Learning Algorithms for Optimal Monitoring in Multi-Channel Wireless Networks,” IEEE Transactions on Wireless Communications, vol.13, no.2, pp.1023-1033, February 2014.

[15] N. Tsikoudis, A. Papadogiannakis and E. P. Markatos, ”LEoNIDS: a Low-latency and Energy-efficient Network-

level Intrusion Detection System,” IEEE Transactions on Emerging Topics in Computing, Vol. PP, no. 99, 2014.

[16] R. Muradore and D. Quaglia, ”Energy-Efficient Intrusion Detection and Mitigation for Networked Control Systems Security,” IEEE Transactions on Industrial Informatics, Vol. 11, no. 3, pp. 830-840, 2015.

[17] S. Shen, ”A game-theoretic approach for optimizing intrusion detection strategy in WSNs,” Proc. 2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), pp.4510-4513, 8-10 Aug. 2011.

[18] A. Afgah and S. K. Das and K. Basu, ”A Non-cooperative Game Approach for Intrusion Detection in Sensor Networks,” Proc. VTC 2004, Fall 2004.

[19] T. Alpcan and T. Basar, ”A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection,” Proc. 43rd IEEE Conference on Decision and Control, December 2004.

[20] Y. Liu, H. Man and C. Comaniciu, ”A Game Theoretic Approach to Efficient Mixed Strategies for Intrusion Detection,” Proc. IEEE International Conference on Communications (ICC 2006), 2006.

[21] Y. Liu, C. Comaniciu and H. Man, ”Modeling Misbehavior in Ad Hoc Networks: A Game Theoretic Approach for Intrusion Detection,” International Journal of Security and Networks, vol. 1, no. 3-4, 2006.

[22] L. Chen and Jean Leneutre, ”A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks,” IEEE Transactions of Information Forensics and Security, vol. 4, no. 2, June 2009.

[23] A. Patcha and J. Park, ”A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks,” International Journal of Network Security, vol. 2, no. 2, pp. 146-152, March 2006.

[24] N. Zhang, W. Yu, X. Fu and S. K. Das, ”Maintaining Defender’s Reputation in Anomaly Detection Against Insider Attacks,” IEEE Transactions on Systems, Man, and Cybernetics-Part B:Cybernetics, vol 40, no. 3, June 2010, pp. 597-611.

[25] P. Michiardi and R. Molva, ”A Game Theoretical Approach to Evaluate Cooperation Enforcement Mechanisms in Mobile Ad Hoc Networks,” Proc. WiOpt 2003: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, March 2003.

[26] A. Afgah, S. K. Das and K. Basu, ”A Game Theory based Approach for Security in Wireless Sensor Networks”, Proc. International Performance Computing and Communications Conference (IPCCC), April 2004.

[27] S-K. Ng and W. K. G. Seah, ”Game-Theoretic Approach for Improving Cooperation in Wireless Multihop Networks,” IEEE Transactions on Systems, Man, and Cybernetics-Part B:Cybernetics, vol 40, no. 3, June 2010, pp. 559-574.

[28] M. F´eleyh´azi, J-P. Hubaux and L. Butty´an, ”Nash Equilibria of packet Forwarding Strategies in Wireless Ad Hoc Networks,” IEEE ransactions on Mobile Computing, vol 5, no. 5, May 2006, pp. 463-476.

[29] F. Li, Y. Yang and J. Wu, ”Attack and Flee: Game-Theoretic-Based Analysis on Interactions Among Nodes in MANETs,” IEEE Transactions on Systems, Man, and Cybernetics-Part B:Cybernetics, vol 40, no. 3, June 2010, pp. 512-622.

[30] J. Lemaire, ”Cooperative Game Theory and its Insurance Applications,” Astin Bulletin, Vol 21. No. 1.

[31] B. Peleg and P. Sudholter, ”Introduction to the Theory of Cooperative Games,” Second Edition, Springer, 2007.

[32] E-Y. Gura and M. B. Maschler, ”Insights into Game Theory,” Cambridge University Press, 2008.