International Journal of Control Theory and Applications

ISSN : 0974–5572

Volume 9 • Number 40 • 2016

Intrusion Detection in Mobile Ad Hoc Networks using Probability of Genuineness

Snehalatha.N[a] T.S. Shiny Angel[a] Aritra Ganguly[a] and Sandeepan Mukherjee[a]

[a]*Department of Software Engineering, SRM University, Chennai, Tamil Nadu.*

Abstract: A [1] mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. MANETs have distinct advantages over traditional networks in that they can easily be set up and dismantled, apart from providing flexibility as the nodes are not tethered. Mobile advert hoc Networks (MANET) are self-configuring, infrastructure less, dynamic wireless networks in which the nodes are useful resource constrained. Efficient schemes for analyzing and reducing the time duration for which the intrusion detection techniques need to stay active in a cell advert hoc network.

Keywords: *MANET, Topology, tranceivers.*

1. INTRODUCTION

A [1] mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. MANETs have distinct advantages over traditional networks in that they can easily be set up and dismantled, apart from providing flexibility as the nodes are not tethered. We have proposed an efficient way of using intrusion detection systems (IDSs) that sits on every node of a mobile ad hoc network (MANET). We first present the minimization of the active duration of the IDSs in the nodes of a MANET as an optimization problem. We then described a cooperative game model to represent the interactions between the IDSs in a neighborhood of nodes. Besides being operable as a stand-alone network, ad hoc networks can also be attached to the Internet or other networks, thereby extending connectivity and coverage more importantly to areas where there are no fixed infrastructures. Present and future

MANET applications cover a variety of areas. One important application scenario is vehicular ad hoc network (VANET). VANET is a self-configuring network of moving vehicles (*i.e.*, a vehicle is a node) although the movement pattern of nodes are restricted by the road course, traffic regulations, etc.

Due to the inherent characteristics of a MANET, such as mobility, wireless communication links and lack of any centralized authority, providing security in a MANET is a challenging task. Moreover, security solutions for fixed wired networks are not easily adaptable to mobile wireless networks. One way of providing security to a MANET is intrusion detection, a process of monitoring activities in the system so as to determine whether there has been any violation of security requirements. Intrusion Detection System (IDS) is the mechanism used by the nodes of a network for detection of intrusion and has been classified into two broad categories based on the techniques adopted, *viz.*, (*a*) Signature-based intrusion detection and (*b*) Anomaly-based intrusion detection. In signature-based detection, knowledge about the signatures of attacks is incorporated in the detection system. At the occurrence of an attack, the characteristics of the attack is matched with the signatures included in the IDS. If there is a match, then an attack associated to that signature is said to have occurred. In anomaly-based detection, the IDS does not attempt to find a signature match but searches for anomalous events or behaviour. For instance, it could look out for anomalous behaviour such as dropping of data packets and events such as erratic changes in the routing table.

2. RELATED WORK

This section presents existing related work on efficient usage of intrusion detection systems in a mobile ad-hoc network. In [2], the authors provided a formal study on optimizing network topology for edge-self monitoring in sensor networks with the objective of maximizing the lifetime of the network. The focus is on optimized selection of monitor nodes that monitor communication links to reduce the number of monitor nodes. Though the objective is energy conservation, our work focuses on reducing the active time of the monitor nodes instead of reducing the number of monitor node. While the overall energy consumption may be reduced, some nodes' energy may be depleted sooner than the rest.

The protocol SLAM [3] makes use of special nodes called guard nodes for local monitoring in sensor networks. Usually the guard nodes remain in sleep mode in the network. Before communicating a node awakens the guard nodes responsible for monitoring its next hop. The main aim of the protocol is to reduce the time a guard node remains awake for the purpose of monitoring malicious activities. We find that there is an interdependence between the nodes while carrying out network monitoring. However, in our proposed work, a node determines the probability with which its own IDS monitors and schedules its monitoring time independent of the other nodes. Moreover, when a large number of communication links are in use, almost all the guard nodes in SLAM might be awake, which is also a downside of the protocol.

In [4], a protocol for optimal selection and activation of intrusion detection agents for wireless sensor networks is presented. Only nodes which have the trust value above the trust requirement can activate the intrusion agent to monitor packets and send alert packet to cluster heads. It is a requirement in the protocol for each sensor node to maintain a small trust database of its neighbors and the clustering of sensor nodes. A game theoretic framework for distributed intrusion detection in ad hoc networks which maximizes the network lifetime while ensuring guarantees for the achieved security level is presented in [5]. The authors assume that the network in divided into clusters of nodes among which some are trusted. A trusted node is equipped with a perfect IDS so that when it performs intrusion detection, it is effective for the whole cluster and no other node is involved in the monitoring process. In comparison, in our proposed approach we neither assume that some nodes are trusted nor that an IDS is perfect. The existence of the energy security trade-off that is shown in [5] is also observed in our simulation results. More importantly, all the above work ([2]-[5]) assume the network to be static while our approach works even when the nodes are mobile.

In [6], a technique is presented which optimally selects a subset of nodes in a dynamic network, each of which manages/monitors a subset of nodes with the aim of reducing monitoring traffic or choosing nodes predicted to be long-lived. Optimal selection of m out of M sniffers and assignment of each sniffer to one of the K channels to maximize the total amount of information gathered in a multi-channel wireless network is done in [7]. However, our work does not share the same goal as the above two. Reduction of energy consumption by intrusion detection systems is being researched in the context of wired networks too ([8]-[9]). In [8], an architecture (LEoNIDS) is presented for network-level intrusion detection system which resolves the energy-latency trade-off by providing both low power consumption and low detection latency at the same time. Packet-based selective encryption is used in [9] for reducing the energy consumption during intrusion detection for networked control systems security. Game theory is widely used for modeling intrusion detection in wireless networks ([10]-[17]). Several other game-theoretic solutions are also found in the literature that take care of issues like cooperation and selfishness of the nodes in a network ([18]-[21]).

3. PROPOSED SYSTEM

In the existing system the network is not utilized properly and there are some limitations in case of security or the efficient use of the node's resources. Moreover in the existing system does not verify whether the intruder is genuine or not on which our algorithm probability of genuineness is based.

3.1. Overall Description

We present simulation results for the Algorithm and discuss its performance. We design cooperative IDS and deploy it in a MANET simulated using ns2 simulator and compare its performance under two scenarios: 1.We keep IDSs running on mobile nodes in a network throughout the simulation time. 2. We use the Probability of genuineness to confirm the intruder is a genuine one. The basic system architecture is shown in Fig. 1.

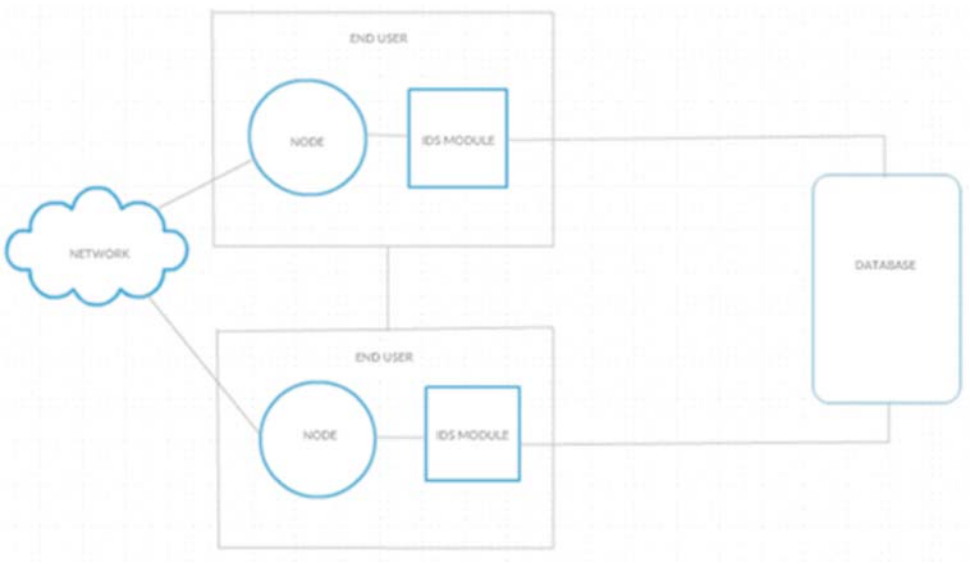

Figure 1

The focus is not on the design of the cooperative IDS but on how integrating the genuineness factor helps reduce the active time of individual IDSs while attempting to maintain its effectiveness. The performance metrics are detection rate, false detection rate, and the saving of energy and computational resource. Additionally, we show the comparison of energy depletion of the individual nodes in the network. We design an IDS, which detects the dropping of data packets, i.e., gray hole attack. A malicious node drops every data packet that comes

its way instead of forwarding it. An IDS sits on every node of the network, where the routing protocol used is AODV (Ad hoc On-Demand distance vector) and the MAC protocol is 802.11. A node obtains the degree of its neighbors with the help of HELLO messages. Each node monitors its neighbors for malicious activities, which we assume here as dropping of data packets. A fixed-size interval, called IDS-interval is used by all nodes. Each node divides the simulation time into slots of IDS-interval (2sec in our case) independently.

2.2. Routing Protocol [AODV]

AODV is an ad-hoc on demand routing protocol designed for operation of mobile ad hoc network providing self-starting, dynamic, loops free, multi-hop routing [22, 23]. This protocol allows the mobile nodes to establish routes quickly for new destinations as well as to respond to changes in network topology and link failures. Nodes do not maintain routes to the destinations that are not in active communication. New routes are created on demand. It means that control packets are broadcasted whenever needed and hence eliminating the need for periodic broadcast of routing updates. AODV protocol works in two phases namely route discovery and route maintenance. Route discovery process uses RREQ (route request) message and RREP (route reply) message. The routing messages contain information about the source and the destination. When a route to destination is needed, the node broadcasts a route request packet to its neighbors to find the optimal path. The RREQ message contains route request broadcast ID, destination IP address, source IP address, destination sequence number, source sequence number and Hop Count. Upon receiving the route request message, the intermediate node forwards the RREQ message until a node is found. This node replies back to the source node with a route reply message RREP and discards the RREQ. RREP contains destination IP address, destination sequence number, source IP address.

Identify the victim node and intruder node: Using AODV Routing protocol divide and conquer strategy can be done. Based on this strategy it can identify the victim node which does not forward the packet to the next node. For identification of intruder, protocol made the victim node as suspected node and sends a route request to the suspected node and if there is no reply coming from the node it is conformed as an intruder and alert message about the intruder is sent to all other nodes.

Steps:

Step 1: Initialize source = 1, destination = N

Step 2: Calculate middle = No of hops (source to destination)/2

Step 3: (i) Check the packet has passed the middle node if yes then calculate the new middle form old middle (source = old middle) to destination, goto Step 2

(ii) Otherwise calculate the new middle for source to middle (destination = middle)

(iii) repeat the process assume there is no flow of data then suspect the node may be the intruder .Process whether the middle node is intruder If True Set victim = middle and initiate route discovery process.

Step 4: confirm victim node

Step 5: Process the flow of data in middle node

Step 6: If the flow is delayed, set destination = prev (mid) and go to step 2

Step 7: If the flow is normal set source = next (mid) and go to step 2

Step 8: Stop

This module is focused for sending alter the message to entire node after the victim node has been identified using divide and conquer strategy and is focused in the route redirection, after send an alert message it will redirect the route from source to the destination.

3.3. Algorithm explanation

Let there be an ad hoc environment containing both intruder nodes and non-intruder nodes and x be the estimated life time of the network. The probability for a node to become intruder within the network lifetime time x is given by (1),

$$a = \frac{\text{No. of packets for warded for its neighbours}}{\text{No. of packets received from their neighbours}}, \quad (1)$$

Where 'a' is the probability of genuineness identified for a node. Let y be considered as a random variable used for classifying the nodes in ad hoc scenario as intruder and co-operative based on the value of 'a'. If the value of a reaches below the threshold value of 0.50 as proposed in (1), then the particular node may be called as a genuine intruder. But when the value of 'a' is above the threshold, and then the node is said to exhibit normal behaviour. If a node is with probability (1–a) then it is said to be in normal behaviour. At the same time, the node possesses intruder behaviour with the probability 'a', given by (2) and (3),

$$P_y(0) = 1 - a, \quad (2)$$

$$P_y(1) = a. \quad (3)$$

Then, the random variable (y) is defined as $y = 0$, if a node exhibits normal behaviour $y = 1$, If a node exhibits intruder behaviour let us assume that the network contains (n) nodes, in which there are 'm' cooperative nodes as well as ($m - n$) intruder nodes. Then, the probability for a node to exhibit normal behaviour (λ) is given by (4) and (5),

$$\lambda = \frac{m}{n}(1-a) + \frac{m-n}{n}a. \quad (4)$$

Under the condition,

1. 'm out of n' nodes are co-operative with probability (1–a) and
2. (m–n) out of n nodes are intruder with probability 'a'.

Thus,

$$\lambda = \frac{m - na}{n}. \quad (5)$$

Since, the network lifetime x could be expressed as the sum of two independent exponentially distributed random variables, each of parameter λ. Thus, the failure rate of co-operative nodes in any time t is given by (6),

$$f_{x/y}(y=0) = \lambda e^{-\lambda t} \quad (6)$$

$$f_{x/y}(y=1) = \lambda^2 t\, e^{-\lambda t} \quad (7)$$

In contrast, the failure rate of intruder nodes in any time t are Erlang distributed is given by (7),

Since, Erlang distribution is a kind of phase type distribution which depends upon sum of independent exponential random variables. This distribution is considered for identifying the failure rate network. In this scenario, the failure rate of entire network depends on the failure rate of co-operative nodes as well as intruder nodes with probability of (1–a) and (a) respectively. Hence, the failure rate of entire network is given by (8),

$$f_{x/y}(y=0) + f_{x/y}(y=1) = \lambda(1-a)e^{-\lambda t} + \lambda^2\, ate^{-\lambda t} \quad (8)$$

Thus, the Erlang based Conditional Reliability Coefficient (ECRC) for identifying the impact level of intruder nodes on the network at any time t is given by (9)

$$R_{x/y}(t) = (1 + a\lambda t)e^{-\lambda t} \quad (9)$$

In general, the level of impact of intruder nodes on the resilience of the network could be identified based on the values of ECRC. If the ECRC value is nearer to zero, then the impact of intruder is less. In contrast, when the ECRC value diverges from zero, then the impact of intruder increases significantly. This Erlang based Conditional Reliability Coefficient Model also aids in framing an optimal range for detecting intruder nodes. The proposed mechanism is a distributed model deployed in each and every mobile node of the ad hoc environment.

4. SIMULATION AND PERFORMANCE

Network simulator [24] or ns is a name for a series of discrete event network simulators, specifically ns-1, ns-2 and ns-3. All of them are discrete-event computer network simulators, primarily used in research and teaching. ns-3 is free software, publicly available under the GNU GPLv2 license for research, development, and use. The goal of the ns-3 project is to create an open simulation environment for computer networking research that will be preferred inside the research community.

1. It should be aligned with the simulation needs of modern networking research.
2. It should encourage community contribution, peer review, and validation of the software.

Now we have 3 screenshots namely Fig. (2, 3 and 4) which shows different time period of the simulation. Fig. 2 shows a new node is trying to enter the network. Fig.3 shows that the new node which was trying to enter (shown in Fig. 2) the network has now successfully connected to the network and is communicating with others. And finally in Fig. 4 the intruder is found in the network.

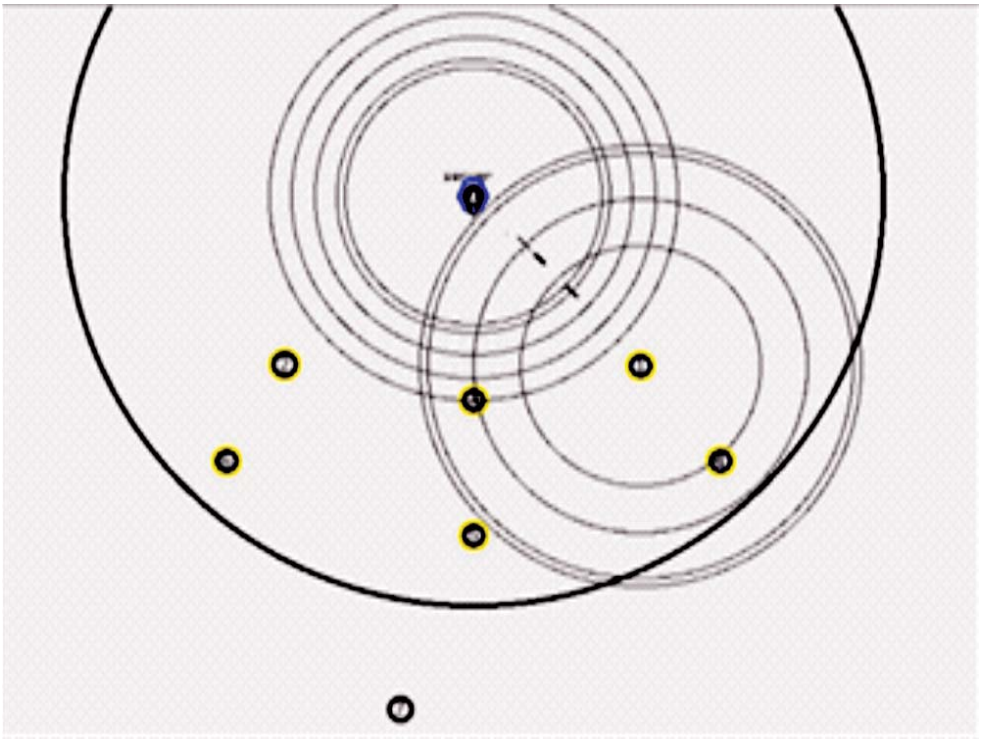

Figure 2

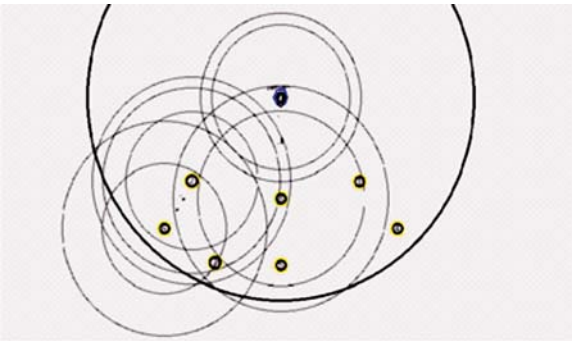

Figure 3

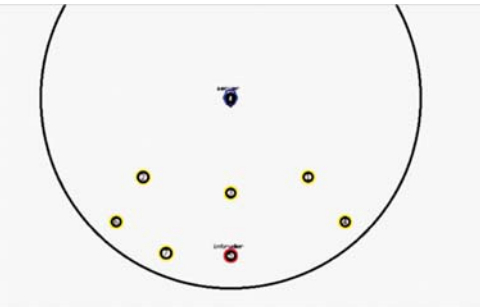

Figure 4

Figure 5

The performance of the IDS system is through the proposed model and algorithm is shown by the detection rate graph [Fig. 6] and the genuineness graph [Fig. 5]. Now both the graphs show that the proposed model is a better one. The detection rate graph shows the difference in detection of the intruder while using both the techniques. The genuineness graph shows the result on basis of correct packet transfer. In both Fig.5 and Fig.6 the existing graph is for LDK algorithm and the proposed graph is by using Probability of genuineness.

Figure 6

5. CONCLUSION

Intrusion detection systems (IDSs) that sits on every node of a mobile ad hoc network (MANET). We first present the minimization of the active duration of the IDSs in the nodes of a MANET as an optimization problem. We then described a cooperative game model to represent the interactions between the IDSs in a neighborhood of nodes. The game is defined in such a way that the primary goal of the IDSs is to monitor the nodes in its neighborhood at a desired security level so as to detect any anomalous behavior, whereas, the secondary goal of the IDSs is to correctly detect the genuine intruder in the system.

REFERENCES

[1] https://en.wikipedia.org/wiki/Mobile_ad_hoc_network

[2] 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.

[3] 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.

[4] 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.

[5] S. M. Fitaci, K. Jaffres-Runser and C. Comaniciu, "On modeling energy security 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] Perkins, C., Belding-Royer, E., Das, S.: Ad-hoc on-demand distance vector (aodv) routing, rfc- 3561, network working group (July 2003).

[23] Perkins, C.E., Royer, E.M.: Ad hoc on-demand distance vector (aodv) routing. In: Proceeding of IEEE Workshop on Mobile Computing system and applications. pp. 90-100 (February 1999).

[24] https://en.wikipedia.org/wiki/Ns_(simulator)