Analysis of Game Theory Technique for Net-Centric Security Applications

Alok J Shukla[1], Dr.Manju Nanda[2], Kushal K S[2]
[1]Manipal Institute of Technology, Manipal, India
[2]CSIR National Aerospace Laboratories, Bangalore, India
alokjs89@gmail.com, manjun@nal.res.in, ksk261188@gmail.com

ABSTRACT— Net-centric Operations (NCO) including Net-Centric Warfare (NCW) has taken a paradigm shift in a way wars are fought involving intelligence, strategic decision making and deploying strategies which can effectively be demonstrated by probabilistic mathematical model known as 'Game Theory'. In this paper the proposed work models the agent behavior which are represented by two players of a game one is a source/victim node and another being an intruder/attacker node initiates a game by deploying mixed strategies. The main idea is to tackle intruders for the benefit of the network by not purging it out of the network once it is being detected as intruder. The scenario of two-player non-cooperative zero sum game in a Wireless Mesh Network Setting is demonstrated wherein the payoff of the players which is the utility of the source/attacker is examined with varying dropping probability of packets and forwarding probability of packets through results. The scenario considered is theoretical model wherein an attacker/intruder is performing selective forwarding attacks.

Index Terms—Game Theory, Players, Strategies, Payoff, Utility, Wireless Mesh Network, Intrusion Tackling, Selective Forwarding.

I. INTRODUCTION

Security for Net-Centric Warfare (NCW) adopted in Cyberspace is more than conventional cryptographic techniques like CIA (Confidentiality, Integrity and Authentication) and is also about mathematical modelling techniques for understanding behaviour of agents, decision making and intelligence in carrying out effective mission strategies on the go successfully by the military forces deploying Mobile Ad-Hoc Networks (MANETs) specially the military deploy hybrid tactical Wireless Mesh Network (WMN) for carrying out Net-Centric operations (NCO).

Net-Centric Warfare (NCW) is a military doctrine/hypothesis [1] that supports the use of data age ideas to accelerate information interchange and upgrade situational awareness through system administration and thus enhancing both the proficiency and adequacy of military operations. Air force is the one among the three defense forces that have embraced Net-Centric operations the most [2].

Net-Centric Warfare includes on how dispersed forces achieve information superiority from information aggregated through use of smart sensors and information being routed in a data centric fashion among peer nodes. Data prevalence is extremely basic prerequisite for net-centric operations in fighting as the necessities for both commanders and warriors has expanded which incorporates continuous video surveillance involving Global Positioning System (GPS). Fighting elements form a networked grid communicating information on the go through a fast paced communication.

The military use mesh networking with a self-configuring topology called as "Ad-hoc" networks for its ease of installation and low-cost and mainly it possesses self-healing property [3]. The military/defense organizations operate in cyberspace where critical insider information of wars or next tactical moves are shared which could be breached.

Cyberspace will play a dominant role where none of the involved entities is assured to hold information dominance in terms of intelligence and accessibility in future warfare. Hence, a game-centric approaches involving collaboration and compelling moves need to be played effectively. Then the question is how such a game-centric approach can be constructed in cyberspace? The answer to this question is that a game-centric approach with minimum two players needs to be placed which is a legitimate player and another is an attacker. A success of an individual player is dependent on the choices made by other players who are involved in the game [4].

Game theory in context of network security tackles with issues where numerous players with opposing objectives and motives compete with/against each other. Here in this scenario, a non-cooperative game is considered where one player wins and other player loses. It equips us with the mathematical framework for analysing, modelling agent behaviours, actions dealing with network security problems.

Here in this proposed work game theory is applied to tackle intruders uniquely from conventional Intrusion Detection Systems (IDSs) where the intruders who cause harm to the network are handled in such a way that they are made to stay in the network by providing utility in the form of incentives/profit but later they are utilized to do good for the network if the intruder happily agrees to stay in the network else it is purged out of the network immediately [5]. A mathematical model involving mixed strategies of two players payoff is realized and in mixed strategy set of both the players, their moves is unpredictable or random. All the parameters of the mathematical model are chosen randomly based on assumptions and considerations to obtain simulation results.

II. LITERATURE SURVEY

Till date, the research contributions in the area on intrusion in Wireless Mesh Networks (WMNs) has not been significant. In many occasions the works carried out doesn't provide optimal solution to the underlying problem but provides some kind of vague overview.

The works proposed in [6] brings out an algorithm to defend specifically against security attacks in WMNs where it uses counter threshold to find the threshold value. This threshold value computed is checked with the original number of data packets sent. The route is declared to contain malicious nodes if the original number of data packets is lesser than the threshold value, which even signifies the packet loss is due to malicious nodes. Hence, the path will be eliminated from the route. This method is not efficient to tackle security attacks in dynamic topologies of WMNs and works on specific settings only.

Authors in [7] propose an authentication protocol for accessing network (PANA) to authenticate wireless clients. The PANA model provides the cryptographic tools required to create an encrypted tunnel with the concerned remote access router. However, the mechanism of authentication is tedious, cumbersome and resource consuming which is safeguarding the confidentiality of exchanged information and the approach as a whole is analysed, it has not been significantly tested meticulously that could persuade the reviewers and readers about the robustness, efficiency in practical implementation scenarios.

Authors in [8] present a novel algorithm called channel-aware detection (CAD) which adopts two different tactics to detect grey hole attacks. Their approach detects a potential victim mesh node by hop-by-hop loss observation and traffic overheating.

Much of the efforts and focus has been spent on investigation and researching on the utilization of cryptographic techniques, protocols to secure the information being transmitted enroute the wireless network. Many such trivial and fundamental solutions have been addressed and put into practice in ad-hoc WMNs to mitigate various kinds of malicious attacks as discussed in [9], [10], and [11].

Authors in [12] put forward a framework of a non-cooperative zero-sum game between legitimate and malicious mesh routers and utilize mathematical tools and models for their approach. The game model proposed in this literature mitigates the issue of grey hole attacks wherein the malicious node drops a subset of the packets it receives from the victim/target node. The game involves a source node as target and malicious node as the attacker node, each of the two nodes competes with one another for finite resources and each individual nodes gains/wins based on its own strategy and that of the other. The attacker is benefitted when packets are dropped and the target is benefitted when packets are forwarded successfully.

In the proposed approach in this paper dwells around same idea and adopts a game theoretic model on the same lines as part of total solution to the problem identified. However, the deviation or the uniqueness adopted in proposed methodology in this paper is in the fact that solution circumvents the flaws of the work in [12] by using our own mathematical model of tackling intruders and choosing parameter values appropriately.

Authors in [12] as an example to illustrate chooses 50% of the packet arrival rate to send buffer based on which gain both nodes vary. Hence, it is considered to be impractical since in reality, packet rates are considered to be higher to significantly reduce packet delays and a huge number of nodes must be involved in communication in any WMN.

The proposed intrusion tackling model discussed in paper and [12] is closely related wherein selective forwarding attackers are detected and isolated in multi-hop network scenarios by comparative performance analysis. The analysis of the misdetection probability or false alarms is carried out and a design is brought to minimize these to a particular threshold. However, the concept is complicated, pays attention on a small range of attacks, and is feasible only in few restricted scenarios. The literature in [12] essentially pays much attention on the signalling and communication part in the physical layer and is in many ways related to our approach undertaken which becomes the motivational aspect in formulation of our approach.

III. METHODOLOGY

The security model for is performing intrusion tackling [5] in place of direct intrusion prevention in WMNs. A hybrid wireless mesh network is assumed where various kinds of devices form the boundary part or could manifest the role of clients. The setting of wireless mesh network is shown in **Fig.1.**below. It consists of mesh routers and mesh clients, where mesh routers form the backhaul providing both mesh and conventional client's network access. Mesh clients can connect among themselves or to centralized backbone. Hence the mesh router forms a means of communication for mesh client to access the network in a multi-hop fashion.

978-81-933187-0-6 © 2018 SEEEPEDIA.ORG
Society for Engineering Education Enrichment

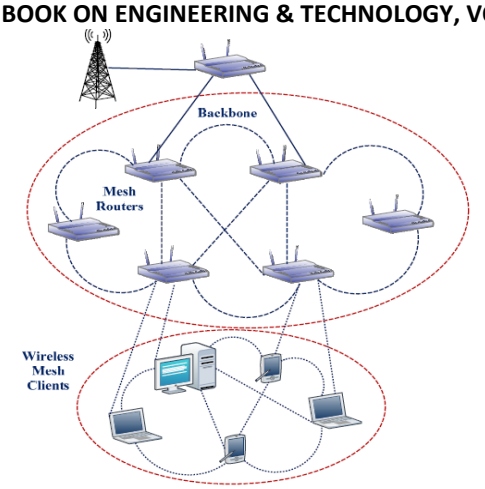

Fig. 1. Setting of Wireless Mesh Network

A careful observation of the **Fig.1.** Reveals nodes in the perimeter of the network are mobile which permits the intruder to tinker the information in the network. The assumption is that standard security mechanisms are present within the network. The primary intrusion detection agents are installed in any node of the network. The proposed mechanism comes into effect after an intrusion is detected or some node is being suspected of being an intruder. Here rather than purging the intruder out of the network immediately after an attacker has intruded into the network directly as in conventional intrusion detection systems, the model proposed is interested in dealing with the intruder if it is suspected to be such.

Fig.2. below shows the operational flow diagram of proposed intrusion tackling model. The intrusion database could be stored in any of the devices with enormous storage space or could be partially maintained by each of the nodes. Here each of the node serves as intrusion tackler for its neighboring nodes.

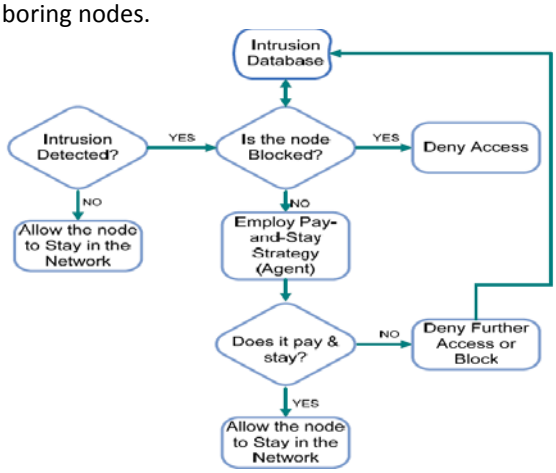

Fig. 2. Operational flow diagram of intrusion tackling model

The main goal of bringing out our model is to maximize or save the utilization of the network resources by applying the burden of transmission of packets on a rogue entity. If the rogue entity denies to render service, the proposed intrusion tackling model purges the intruder out from the network, and this is how our proposed mechanism deals with an intruder in a wireless mesh network setting by game theoretic approach which is mathematically modelled and is realized by implementing in MATLAB [15].

There are mainly two phases in the approach of intrusion tackling. The first phase is tackling intruders based on game theoretic technique and second phase is detecting intruder by marking and taking a decision which is a part of intruder tackling model which is achieved using Wireless multi-hop acknowledgement algorithm.

A. Strategy Initiation to put forth a Competition by game theoretic technique

Game theory [13], [14] can be characterized as measurable model to investigate the association between the gatherings of players who act deliberately. Fig.3. below shows our proposed intrusion tackling model for handling intruders where two players are considered Player_1 who is source/target victim mesh node and Player_2 is intruder/attacker with a bad intention performing selective forwarding of packets and whose aim is to damage to whole network by degrading the payoff player_1.

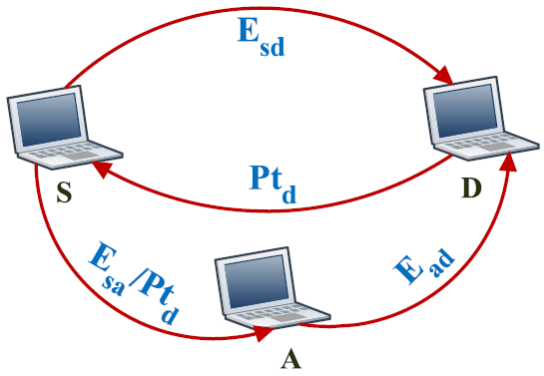

Fig. 3. Mathematical model of our intrusion tackling mechanism consisting of two players S and A.

Before presenting the mathematical model of our approach. **Table I gives** an overview of the notations used in the mathematical equations leading to the formulation of mathematical model represented as resultant payoffs in form of utility functions of source node and attacker node.

TABLE I. BASIC NOTATIONS AND THEIR MEANINGS IN INTRUSION TACKLING MODEL

Notation	Meaning
p_i	Probability to defend the ith node in the network
v_i	Intermediate mesh node
V_{i-1}	Upstream mesh node
V_{i+1}	Downstream mesh node
μ	Packet arrival rate
E_{sd}	Energy spent for utility cost
E_r	Remaining energy
α	constant
p_a	Probability of transmitting packets via Player_2
p_d	Probability of direct transmission of packets
q_f	Forwarding probability
q_d	Probability of dropping the packet
P_t	Points received

978-81-933187-0-6 © 2018 SEEEPEDIA.ORG
Society for Engineering Education Enrichment

Assuming or we shall assign probability p_i for defending ith node in the network. Total probability of defending all N nodes is $\sum_{i=1}^{N} p_i$. The energy utilized for utility metric cost is given as: $E_{sd} = \sum_{i=1}^{N} p_i$.

The pending energy is given by: $E_r = 1 - E_{sd}$ where $E_{sd} <= 1$. The motive here is energy that attacker utilizes to cause havoc to the network should be greater than the energy spent by the victim.

The game possess 4 states in the form (m,n), where m denotes the transmitting buffer of source node i.e., Player_1 and n denotes the discarding pool buffer of attacker/intruder node i.e., Player_2. Here m will possess a value of 1, when there is a packet to transmit on the transmitting buffer of player_1 and n will take values of 0 or d depending on packets being dropped or not. Let μ be the rate of arrival of packets at the transmitting buffer of source node and it is assumed to happen at a fast rate. The possible four states possessed by the game are as follows: $g_1=(0,0)$, $g_2=(0,d)$, $g_3=(1,0)$, $g_4=(1,d)$.

This being a stochastic model we need to compute transition probabilities from one state to another, that is computation of current state given previous state and computation of future state knowing past and current state with different probabilities that multiplied by utilities of source and attacker which are their individual payoffs formulated from their individual random strategic sets of forwarding/dropping behavior we compute the model.

When there is a packet in sending buffer of Player_1, possible transition probabilities of states of game involving mixed strategies:

$$P_{(m,n)(m+i,n)}(x) = \begin{cases} (1-\mu)(p_d + p_a q_f) & \text{;if i= -1, n=0} \\ (1-\mu)(p_a q_d) & \text{;if i= -1, n=d} \\ \mu(p_d + p_a q_f) & \text{;if i= 0, n=0} \\ \mu(p_a q_d) & \text{;if i= 0, n=d} \end{cases}$$

When there is no packet in sending buffer of Player_1, possible transition probabilities of states of game involving mixed strategies:

$$P_{(m,n)(m+i,n)}(x) = \begin{cases} (1-\mu) & \text{; if i=0, n=0} \\ \mu & \text{; if i=1,n=d} \end{cases}$$

where, μ is the rate of arrival of packets in the transmitting buffer and x is the mixed strategies of two players.

The payoff of Player_1 is $S_1 = \{S_1, S_2\}$ which implies that player_1 sends the packets directly to destination D (S_1) or via A (S_2). Mixed strategies where strategies are deployed randomly with a unknown probabilities is denoted by x correlated to S_1 are $\pi_s(S_1,S_2) = (p_d, p_a)$, where $p_d + p_a = 1$. On the same lines the strategy set for Player_2(attacker node) relates to A_2 are $\pi_a(a_1, a_2) = (q_f, q_d)$ where $q_f + q_d = 1$. Here q_d = probability of dropping the packet. Hence, $(\pi_s, \pi_a) = (p_d, p_a, q_f, q_d)$.

The destination node yields utility in the form of profit or points to source S for the transmitted packet. When source node S routes packets along the path S→D, node S procures some points as utility of Pt_d from D. When S routes packets through A, it procures modified points replaying packets and procures points Pt_d from D and gives A points or reward/benefit to stay in network of Pt_{sa}. If S doesn't procure any points/reward from D for the transmitted packet, it signifies the packet didn't get transmitted successfully to D. For each transmission of packets in a wireless medium from intermediate node to downstream node will cause an energy exhaustion of E v_i V_{i+1}. Hence based on the energy exhausted and rewards procured the source/victim and attacker nodes S and A will sustain with the following net utility functions:

$$U_s = \begin{cases} Pt_d - E_{sd}; & \text{S forwards packets directly to D} \\ Pt_d - Pt_{sa} - E_{sa}; & \text{S forwards packets to D via A.} \\ -Pt_{sa} - E_{sa}; & \text{node A drops the packet.} \end{cases}$$

If $(-Pt_{sa} - E_{sa}) < (Pt_d - E_{sd}) < (Pt_d - Pt_{sa} - E_{sa})$, the utility of S decreases if A performs dropping of packets compares to utility it procures when a packet is routed to D directly.

$$U_a = \begin{cases} Pt_{sa} - E_{ad}; & \text{A forwards the packet to D.} \\ Pt_{sa} + \beta; & \text{node A drops the packet.} \end{cases}$$

Where β is the profit gained by node A. If $(Pt_{sa} - E_{ad}) < (Pt_{sa} + \beta)$, the utility procured from discarding the data packet is greater than the utility procured from S for forwarding the packet.

The overall utility can be calculated from the equations below which is result of product of probabilities and the payoffs representing the strategic moves which are random. Based on these two equations formulated results are obtained in MATLAB.

$$U_s(x) = \mu(1-\mu p_a q_d)\{p_d(Pt_d - E_{sd}) + p_a(q_f(Pt_d - Pt_{sa} - E_{sa}) + q_d(-Pt_{sa} - E_{sa})) + \mu^2 p_a q_d\{p_d(Pt_d - E_{sa}) + p_a(q_f(Pt_d - Pt_{sa} - E_{sa}) + p_a(q_f(Pt_d - Pt_{sa} - E_{sa})) + p_a(q_d(-Pt_{sa} - E_{sa}))\}$$

$$U_a(x) = \mu(1-\mu p_a q_d)\{p_a(q_f(Pt_{sa} - E_{ad}) + q_d(Pt_{sa} + \beta))\} + \mu^2 p_a q_d\{p_a(q_f(Pt_{sa} - E_{ad}))\} + \mu^2 p_a q_d(p_a q_d(Pt_{sa} + \beta))$$

B. Multi-hop acknowledgement based algorithm for malicious node(s) detection

The model proposed comes into picture once the intrusion event happens and not prior to the intrusion event. Now question is how to identify the intruder? For this question, a multi-hop acknowledgement algorithm is proposed to detect malicious nodes acting as intruders by analyzing their behaviors which are carrying out selective forwarding attacks. This algorithm marks the intruder by hop-by-hop loss observation and traffic overhearing mechanisms.

Algorithm:

Parameters: v_{i-1} (downstream node), v_i (Intermediate node), v_{i+1}(Upstream node).

Do

Begin

Initailize

Packet counter =0;

$v_{i+1} \leftarrow v_{i-1}$

Update v_{i+1}

Packet counter←packet sequence number +1;

Packet counter++;

978-81-933187-0-6 © 2018 SEEEPEDIA.ORG
Society for Engineering Education Enrichment

For packet sequence number=0; packet sequence number<toal number of packets received; packet sequence number++
Begin
Delay (link_ACK+packet_Arrival_Time)
End for
Forward: v_i to $v_{i+1;}$
While (packet sequence number==NULL)
End do while

At the Upstream Node: Buffering & overhearing of downstream traffic
Overhears the traffic going to downstream node & makes a decision by making simple analysis.
Operations:
Packet is relayed to downstream traffic by Mesh Router at the Upstream Node

Upstream node

- Buffer ACK & Overhears downstream traffic
- Check whether downstream node forwarded or tampered with traffic by computing MAC over the packet header+ payload.

At the Downstream Node:
The actual MARKING & DECISION MAKING is done at the downstream node.
The downstream nodes maintain 2 parameters.
They are:

- Propability of ACK - P_{Ack}
- Propability of no ACK (NACK), P_{NAck}
- The probability of ACK(P_{Ack})=1- P_{NAck}
- P_{NAck} is computed as $(n_t + n_{d)}/n_f$

Where n_t=no of tampered packets
Nd= no of dropped packets
Nf=total number of forwarded packets
Two packets namely PROBE packet & PROBE_ACK are used to detect the malicious routers in the data path.

Decision:
The opinion of the downstream node is calculated as follows:

- If (P_{NAck}>t_m)=malicious behaviour
- If (P_{NAck}<t_m) =normal behaviour where t_m is the monitoring threshold which carries values between '0' & '1'.

The behaviour of the node is calculated by determining the loss rate of the packets over the link v_i to $v_{i+1.}$ It is calculated using the formula:

- If ($L_{vi \rightarrow vi+1}$>t_l) malicious behaviour is detected.
- If ($L_{vi \rightarrow vi+1}$<t_l) Normal behaviour is detected.

Where t_l is the loss rate threshold that can take any value between '0' & '1'.
The algorithm will detect the malicious behaviour with higher propability with the lower value of t_l & $t_{m.}$

IV. RESULTS AND DISCUSSION

A. Plots of utility of source node/attacker mesh node vs dropping probability of packets (qd) sent directly from Source node to destination node.

Case1: When dropping probability of packets (pd) is 0.8 and forwarding probability of packets by attacker mesh node (pa) is 0.2

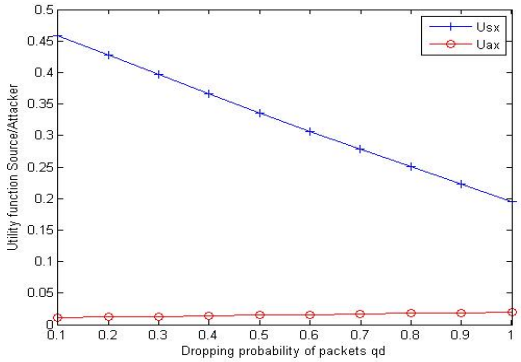

Fig.4. Enhancing the utilities of S as a function of drop probabilities of qd when pd =0.8 and pa=0.2

Case2: When dropping probability of packets (pd) is 0.6 and forwarding probability of packets by attacker mesh node (pa) is 0.4

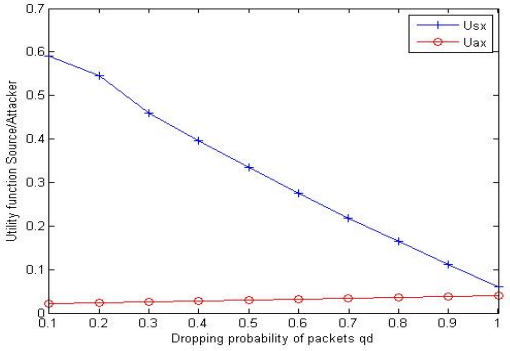

Fig.5. Enhancing the utilities of A and degrading the utilities of S as a function of drop probabilities of qd when pd =0.6 and pa=0.4

Case3: When dropping probability of packets (pd) is 0.4 and forwarding probability of packets by attacker mesh node (pa) is 0.6

978-81-933187-0-6 © 2018 SEEEPEDIA.ORG
Society for Engineering Education Enrichment

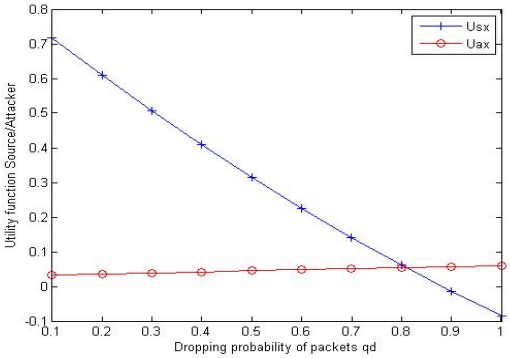

Fig.6. Enhancing the utilities of A and decreasing utilities of S as a function of drop probabilities of qd when pd =0.4 and pa=0.6

Case4: When dropping probability of packets (pd) is 0.2 and forwarding probability of packets by attacker mesh node (pa) is 0.8.

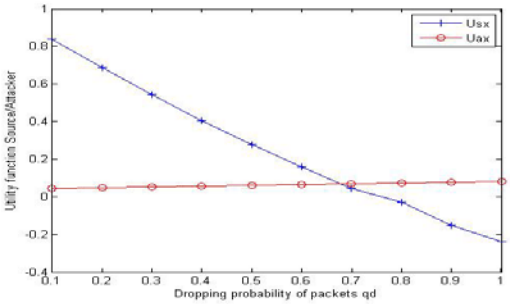

Fig.7. Enhancing the utilities of A and decreasing the utilities of S as a function of drop probabilities of qd when pd =0.2 and pa=0.8

Case5: When dropping probability of packets (pd) is 0 and forwarding probability of packets by attacker mesh node (pa) is 1

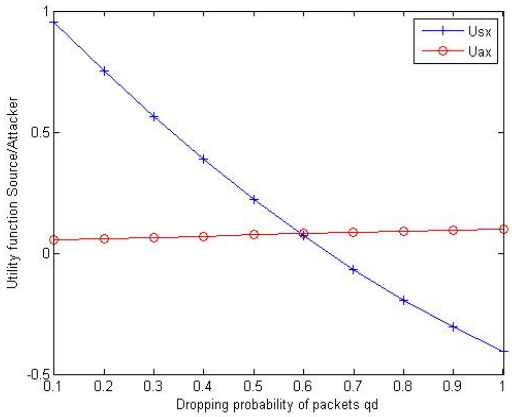

Fig.8. Enhancing the utilities of A and degrading the utilities of S as a function of drop probabilities of qd when pd =0 and pa=1

B. Plots of utility of source node/attacker mesh node vs transmitting probability of packets (pa) sent via Attacker/Player2 from Source node to destination node.

Case6: When probability of forwarding the packets (qf) =1 is maximum and probability of dropping the packets (qd) =0 is minimum transmitted via Player2/Attacker

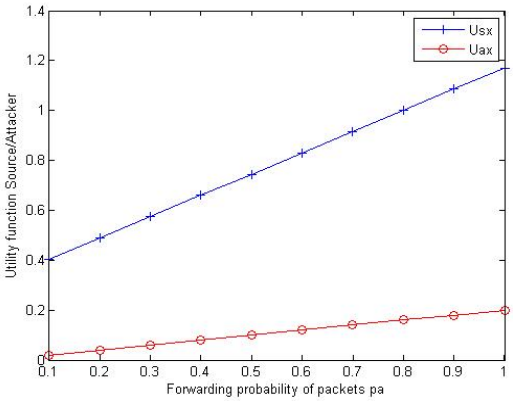

Fig.9. Enhancing the utilities of S and A as a function of forward probabilities pa
when qf=1 and qd=0

Case7: When probability of forwarding the packets (qf) =0.75 and probability of dropping the packets (qd) =0.25 transmitted via Player2/Attacker

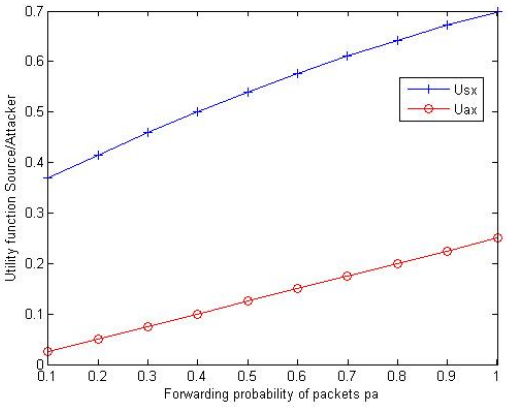

Fig.10. Enhancing the utilities of S and A as a function of forward probabilities pa
When qf=0.75 and qd=0.25

Case8: When both the probabilities of forwarding the packets (qf) =0.5 and probability of dropping the packets (qd) =0.5 transmitted via Player2/Attacker are equal.

978-81-933187-0-6 © 2018 SEEEPEDIA.ORG
Society for Engineering Education Enrichment

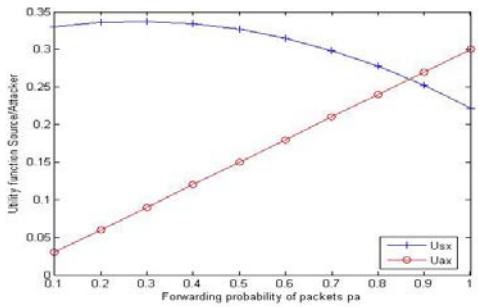

Fig.11. Enhancing the utility of A and degrading the utility of S as a function of forwarding probabilities of pa when qd =0.5 and qf=0.5

Case9: When probability of forwarding the packets (qf) =0.25 and probability of dropping the packets (qd) =0.75 transmitted via Player2/Attacker

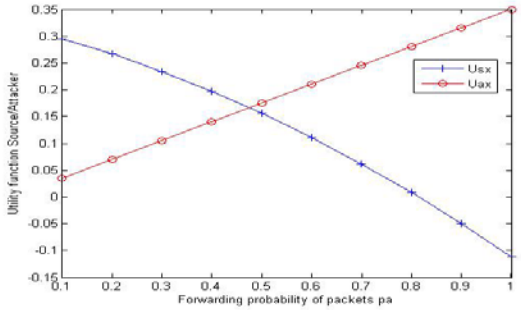

Fig.12. Enhancing the utilities of A and decreasing the utility of S as a function of forwarding probabilities when qf =0.25 and qd=0.75

Case10: When probability of forwarding the packets (qf) =0 is minimum and probability of dropping the packets (qd) =1 is maximum transmitted via Player2/Attacker

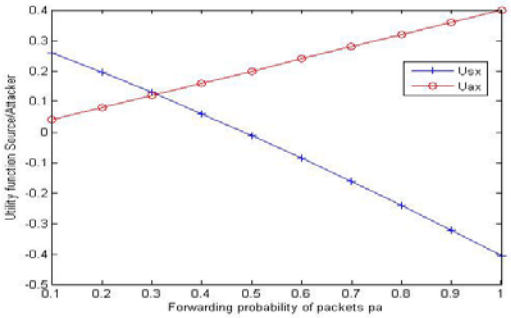

Fig. 13. Enhancing the utility of A and degrading the utility of S as a function of forwarding probabilities of qd when qf =0 and qd=1

V. CONCLUSION AND FUTURE WORK

The game theoretic analysis was carried out for tackling intruders in a Wireless Mesh Network setting using MATLAB programming. The game theoretic analysis was carried out by mathematical modelling of utility functions of source/victim node and attacker nodes. In general, the results shows that the Player_1(source) sending packets in the setting wins when packets are forwarded even when packets are routed through attacker and as dropping probability player_1 increases chances of it winning decreases measured by performance metric like utility function. Player_2 (attacker) wins when packets are dropped when packets are routed through it. The considered game setting is a non-cooperative game where moves of individual of two players are random in nature i.e. mixed in nature. MATLAB plots were used to realize the same for mathematical and programming aspects.

As a future scope of work this model could be applied to a case colluding intruders performing selective forwarding attacks and mathematical model could be developed on the same lines. The model could not fit well with other Mobile Adhoc Networks (MANET's) like Wireless Sensor Networks (WSNs). But Mesh networks could fit with futuristic networking technologies like Ubiquitous Computing/Pervasive Computing, Cloud Computing and Internet of Things (IOT) where there is a way for humans and machines to communicate through smart sensors and deployment of machine intelligence for devices in Netcnetric Operations. It can be applied as game of netcnetric warfare of swarm of UAVs (Unmanned Aerial Vehicles) in a data centric routing environment. For detecting of intruders anomalously, machine learning algorithms could be applied and adversarial search could be performed using artificial intelligence algorithms for game theory.

ACKNOWLEDGMENT

The authors would like to acknowledge the Director of CSIR-NAL, Bangalore for supporting this work.

REFERENCES

[1] R. Koch, "Blackout and Now ? Network Centric Warfare in an Anti-Access Area- Denial Theatre," pp. 169–184, 2015.

[2] M. Maybury, "Toward the Assured Cyberspace Advantage : Air Force Cyber Vision 2025," no. February, 2015.

[3] N. Warfare and W. Communications, "Modern warfare is increasingly network centric," no. 408, pp. 1–4, 2008.

[4] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A Survey of Game Theory as Applied to Network Security "

[5]]A. K. Pathan, S. Khanam, H. Y. Saleem, and W. Mustafa, "Tackling Intruders in Wireless Mesh Networks" in Distributed Networks: Intelligence, Security and Applications, Qurban A.Memon, Ed.FL: CRC Press,2014,pp.167-190.

[6] Shila D.M. and Anjali, T., "Defending Selective Forwarding Attacks in WMNs", IEEE International Conference on Electro/Information Technology 2008 (EIT'08), Iowa, USA, May 18-20, 2008, pp. 96-101.

[7] Nagaraj Balakrishnan, Reshmi S., and R. Arunkumar. "SMART REAL TIME RESCUE SYSTEM FOR FISHERMEN." Pak. J. Biotechnol. Vol 15.1 (2018): 73-75.

[8] Cheikhrouhou, O., Laurent-Maknavicius, M., and Chaouchi, H., "Security Architecture in a Multihop Mesh

Network", 5th Conference on Safety and Architectures Networks SAR 2006, Seignosse, Landes, France, June 2006, pp. 1-10.

[9] Shila, D.M., Cheng, Y. and Anjali, T., "Channel-Aware Detection of Gray Hole Attacks in Wireless Mesh Networks", The Proceedings of IEEE Globecom 2009, Nov. 30 2009-Dec. 4 2009, Honolulu, HI, USA, 2009, pp. 1-6.

[10] Parno, B., Perrig A., Gligor, V., "Distributed Detection of Node Replication Attacks in Sensor Networks", Proceedings of the 2005 IEEE Symposium on Security and Privacy (S&P'05), 8-11 May 2005, pp. 49-63.

[11] Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C., and Belding-Royer, E.M., "A Secure Routing Protocol for Ad Hoc Networks", Proceedings of the 10 th IEEE International Conference on Network Protocols (ICNP'02), 12-15 Nov. 2002, pp.78-87.

[12] Salem, N.B. and Hubaux, J.P., "Securing Wireless Mesh Networks", IEEE Wireless Communication, Volume: 13, Issue: 2, April 2006, pp. 50-55.

[13] Shila, D.M. and Anjali, T., "A Game Theoretic Approach to Gray Hole Attacks in Wireless Mesh Networks", in Proc. IEEE MILCOM, San Diego, CA, Nov. 16-19 2008, pp. 1-7.

[14] Srivastava, V., Neel, J., MacKenzie, A.B., Menon, R., DaSilva, L. A., Hicks, J. E., Reed, J. H., and Gilles, R.P., "Using game theory to analyze wireless ad hoc networks", IEEE Communications Surveys & Tutorials, Fourth Quarter 2005, Volume 7, No. 4, 2005, pp. 46-56.

[15] Javidi, M.M. and Aliahmadipour, L., "Game theory approaches for improving intrusion detection in MANETs", Scientific Research and Essays, Vol. 6 (31), 16 December 2011, pp. 6535-6539.

[16] www.mathworks.com

978-81-933187-0-6 © 2018 SEEEPEDIA.ORG
Society for Engineering Education Enrichment