A Grudger Based AIS Approach to Coerce Selfish Node Cooperation in MANET

Lincy Elizebeth Jim and Mark A. Gregory
(Corresponding author: Mark A. Gregory)

Department of Electrical and Electronics Engineering, RMIT University
124 La Trobe St, Melbourne VIC 3000, Australia
(Email: mark.gregory@rmit.edu.au)

(Received Aug. 14, 2017; revised and accepted Nov. 11, 2017)

Abstract

Mobile Ad hoc Networks (MANET) utilize multi-hop communications to forward packets across the network consuming power, processing, and memory resources. In an ideal MANET the nodes are unselfish and forward packets on demand. The real-time, ad hoc and open characteristics of MANET make it susceptible to selfish and malicious nodes affecting performance. In a MANET, some of the nodes may decide to selfishly cooperate or to not cooperate, with other nodes. The selfish nodes reduce the overall effectiveness of network communications, decrease packet delivery rates and increase packet delivery time. This paper investigates an approach to harness selfish node energy and transmission capacity to share network load. This paper utilizes a Grudger Artificial Immune Systems based trust model to study the impact of selfish nodes in the network. The proposed algorithm demonstrates an increase in the packet delivery ratio.

Keywords: Artificial Immune System; Grudger; Mobile Ad hoc Networks

1 Introduction

In Mobile Ad hoc Networks (MANET) information is sent across the self-organizing network utilizing node to node communications. MANET is an ideal candidate for mobile communications in regions with limited access to fixed infrastructure and for emergency and disaster relief operations. The nodes that form a part of the network have limited battery power and utilize the help of other nodes in the network for packet forwarding. The traditional MANET routing protocols like Dynamic Source Routing (DSR) [1] and Ad hoc on Demand Distance Vector (AODV) [2] function on the assumption that all nodes are highly cooperative and truthful. The dynamic MANET topology and communication demands, particularly as a relay, can take a toll on the limited node battery power, and it is possible that nodes will adopt a selfish stance to prevent further power drain by relay requests. The selfish nodes continue to consume the resources of other nodes while preserving their resources.

Selfish nodes limit MANET performance, and it is reasonable in certain situations to adopt an approach that isolates selfish nodes upon identification or to encourage selfish nodes to change their behavior before isolation is imposed. MANET is a networking approach that can be utilized for disaster management, military and rescue operations. In each of these scenarios, for MANET to be effective there is a need to limit the number of selfish nodes. MANET effectiveness is increased when the nodes within the network are active participants thereby reducing the amount of traffic that is resent due to nodes failing to relay traffic as requested.

This paper is divided into four sections. Section 2 provides a description of earlier work relating to selfish nodes found in the literature. Section 3 provides an overview of the Artificial Immune System (AIS) and selected AIS algorithms. Section 4 describes the proposed Grudger Artificial Immune System framework (GrAIS). In Section 5, simulation results for scenarios with different mission-critical workloads are presented. Finally, Section 6 concludes the paper and outlines future work.

2 Related Work

Routing protocols developed for MANET can be classified as proactive, reactive and hybrid. The effect of node selfishness on routing and node resource utilization efficiency has not been a focus for earlier research. In [3] misbehavior in MANET was first identified, defined and the focus of this work was to alleviate node misbehavior. Research found in the literature appears to focus on how to detect and isolate selfish nodes. This approach does not penalize the selfish nodes nor to coerce the selfish nodes to forward packets. The malicious nodes are rewarded if they're identified and removed from routing paths. In [4] a review of node selfishness in MANET is provided. This paper summarizes existing approaches to dealing with the selfishness problem and the authors provide a proposed solution to mitigate the selfishness problem. The operation of DSR [5] is explored and as energy depletes node selfishness occurs. Various types of selfishness are defined and the problems arising because of selfish nodes co-existing in the network is investigated. In [6] the data flows between MANET nodes are observed and when a selfish node does not forward a packet, the neighbor node waits for a pre-defined threshold number of packet transmission failures to be exceeded before triggering an alarm.

In [7] the impact of selfish nodes on the quality of service in MANET is explored. This work analyses parameters including throughput, average hop count and packets dropped. The hop count increases as the selfish node concentration increases. The authors found that there is an increase in the number of packets dropped along with a significant decrease in throughput as the selfish node concentration increases. In [8] the MANET nodes are encouraged to be altruistic and the nodes are given positive or negative scores depending on their behavior. The altruistic nodes utilize their energy to relay for other nodes but they relay for selfish nodes only once. This approach does not call for the participation of selfish nodes for any communication.

The Combined Immune Theories Algorithm (CITA) [15, 16] utilizes the basic principles of well-known immune theories including the Dendritic Cell Algorithm (DCA), Clonal Selection (CS), and the Negative Selection Algorithm (NSA). Cerri and Ghioni compare this algorithm with the Secure Ad hoc on Demand Distance Vector algorithm (SAODV) and demonstrate its improved performance [14]. DCA is used to obtain contextual information. Dendritic Cells (DC) are associated with a subset of neighboring nodes called elements, which are responsible for DC maturation. Element subsets are monitored using adjacent Immature Detectors (ID), adjacent Mature Detectors (MTD) and Memory Detectors (MMD). During the learning phase the network is configured with trusted nodes, parameters, alarms and the nodes have a set of detectors. The CITA algorithm shows an improved performance regarding the packet delivery ratio in the presence of malicious nodes performing a denial of service attack.

3 Artificial Immune Systems

AIS are adaptive systems inspired by theoretical immunology and observed immune functions, principles, and models, which are applied to complex problem domains [17]. Research into the immune system is gaining in significance due to its unique ability to solve complex issues. AIS research, as a branch of computational intelligence, has attained importance since its genesis in the 1990's. There are, to date, four major AIS algorithms upon which AIS research is based. They are 1) Artificial Immune Networks (AIN); 2) NSA; 3) CS; and 4) Danger Theory and the DCA. The AIS research field combines the Immunology, Computer Science, and Engineering disciplines to solve complex problems. The prominent AIS features include learning, memory and pattern recognition. Forrest *et al.* initially proposed the NSA [18] to differentiate between self and non-self cells based on the generation of T-cells. This approach was originally applied to computer virus detection. Based on the work of Forrest *et al.* variations of the NSA have been formulated keeping in mind the fundamental properties of the original algorithm.

An immune system is the defender of the human body against pathogens. There has been a significant amount of work in recent research about how to use Human Immune System (HIS) [16] concepts to solve complex problems. The HIS is capable of processing information, learning and memorizing salient information. The AIS borrows principles from the HIS and attempts to apply the fundamental concepts to other applications. The primary task of the HIS is to keep the body healthy and protect it from pathogens. The HIS consists of organs, cells, and tissue that work together to identify and attack dangerous invasive threats like bacteria and viruses. In the event of an attack by a pathogen, a series of steps called an immune response is launched, thereby distinguishing, and protecting cells and tissue from harmful pathogens.

The key to a healthy immune system is the ability to make a distinction between self and non-self cells. The immune defenders launch an attack on anything they identify as foreign. Antigens are foreign objects that trigger an immune response. Transplants from another person may also relate to non-self, can lead to an attack by the HIS and, as a result, to limit the probability that this unwanted outcome can occur, masking drugs have been developed.

The AIN model was redefined by Timmis *et al.* [19]. The AIS coterie has produced many versatile sets of immune inspired algorithms to solve real world as well as computational problems. An insight into the mathematical immuno-computing strategies was provided by Tarakanov *et al.* [20].

3.1 Dendritic Cell Algorithm

Steinman and Cohn [21] identified the DC characteristic as an antigen presenting cell. A DC is mainly composed of leukocytes and is present in all tissue. DCs inside the tissues segregate and mature during an appropriate trigger; once they mature they move to secondary lymphoid tissues and present antigen to T-cells to launch an immune response. Immature DCs are found on the body surfaces including the skin and is also found in blood. When the pathogens are identified, captured and processed by the immature DC the DCs migrate to the thymus and spleen where they mature and induce an immune response.

The change of state of the DC [22, 23] is facilitated by the identification of signals such as the pathogen-associated molecular pattern (PAMP), danger signals and apoptotic signals (safe signals) as seen in Figure 1. The signals are described as follows: (1) PAMPs activate the immune response thereby protecting the host from infection; (2) danger signals are released during tissue cell damage, their strength is lower than PAMPs; (3) safe signals are given out when programmed/normal cell death occurs; and (4) inflammatory cytokines are given out when general tissue distress occurs and amplify the effect of the other three signals. The immune response of the T-cell is determined by the corresponding weights of the four signal types. The DCA was proposed by Greensmith *et al.* [24] and combines various signals to investigate the current circumstance of the environment and non-parallel sampling of another data stream (antigen). A fuzzy margin derived corresponding to the concentration of co-stimulatory molecules is an indicator for a DC to stop antigen collection and migrate to a virtual lymph node. The DCA works on the input signals with presumed weights to produce output signals.

The algorithm proposed in [25] consists of the following stages: initialization, update, and aggregation. During the initialization phase, training and initial values are set. The update stage consists of two stages namely tissue update and cell cycle analysis. The DC is designed as a Libitissue server [26]. The cell cycle is a well-defined process that occurs at a user-defined rate. As soon as the antigen data is processed, the process of the cell cycle and tissue updating stops. During the concluding stage, aggregation of the collected antigens occurs together with analysis, and the Mature Context Antigen Value (MCAV) per antigen is derived.

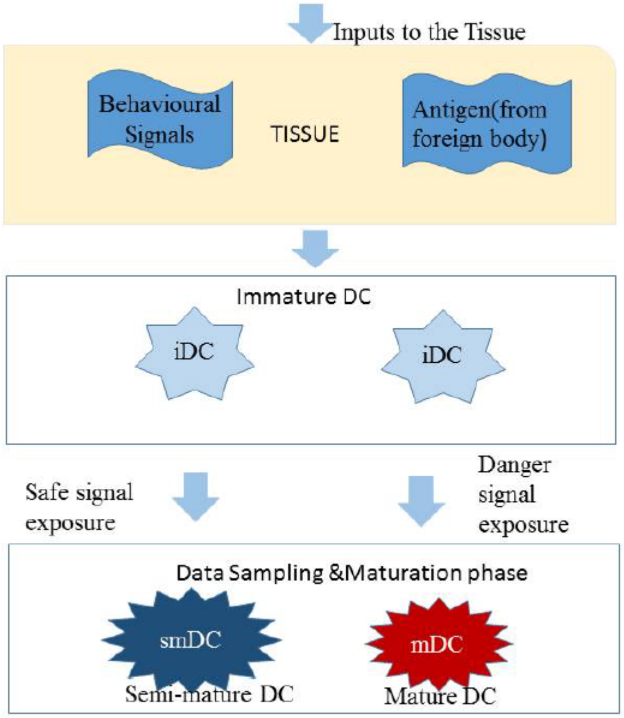

Figure 1: Dendritic cell algorithm schematic

3.2 Danger Theory

The Danger Theory, proposed by Matzinger, emphasized that the "foreignness" of a microbe is not the primary factor that ignites a response [27]. Danger Theory states that antigen-presenting cells are activated by danger/alarm signals from exerted cells. Danger signals will not be sent by robust cells or by cells experiencing normal cell death. Any cell that dies unnaturally sends out a danger signal, and antigens near the dying cell are captured by antigen presenting cells like macrophages and are then dispensed to the lymphocytes. B-cells also secrete antibodies. The antibodies that identify a match with the antigens present in the danger zone will be triggered. Those antibodies that do not identify a match with the antigens will not be in the danger zone and therefore will not be triggered.

The Danger Theory has its drawbacks and Aickelin *et al.* proposed applications of Danger Theory that highlight: (1) the presence of an Antigen Presenting Cell (APC) is crucial for a danger signal; (2) a danger signal does not need to be related to threatening events; (3) danger signals can be positive or negative (presence or absence of signal); and (4) conceptual ideas were also proposed on how the Danger Theory can be used for anomaly detection [29]. Based on the Danger Theory, danger signals always spark an immune response. In a computing application of Danger Theory, low or high memory usage, fraudulent disk activity, and other events could be indicated by danger signals. The immune system reacts to the antigens in the danger zone once a danger signal is created. After the critical components are recognized, they are then sent to a part of the system for further verification. The Two-Signal Model extended by Bretscher *et al.* [28] explains Danger Theory in a different way where two signals are needed to activate the lymphocytes: 1) antigen recognition; and 2) co-stimulation. The co-stimulation signal indicates that the antigen is threatening.

4 Trade-Off Between Selfishness and Altruism

The motivation for this paper stems from the observation that it is not beneficial to the operation of a MANET to ignore or isolate selfish nodes. The approaches presented in Section **??** isolated the selfish nodes with a bad reputation. Initially, all nodes in the network have the same classification and as time changes some nodes tend to become selfish. One of the reasons for nodes to become selfish is due to the relay load that the node may have experienced. Traffic workload has a direct effect on energy consumption and as energy reduces the nodes can become selfish for various reasons including observation of the number and state of neighboring nodes. The good nodes tend to overlook selfish nodes and continue to render service to the selfish nodes irrespective of any service in return. This paper provides a trust model framework that incorporates the good and selfish nodes. The proposal is that for high traffic volumes the routing task should be carried out by all nodes, including selfish nodes. In [11] the author uses a model that considers how birds clean each other of parasites in hard to reach places, therefore helping with individual and group survival. The author defines three different model behaviors:

1) Sucker-Birds that blindly help other birds without expecting anything in return.

2) Cheat-Birds that take advantage of all the help they can get but do not offer anything in return.

3) Grudger-Birds that help others and recall who they have helped. In case the same bird does not reciprocate, they will not help that bird again.

The routing model proposed in this paper categorizes good nodes into a sucker group, cheat nodes into selfish and Dendritic Cell (DC) nodes into a grudger group. In the proposed GrAIS algorithm, as seen in Figure 2, each node is modeled as a Grudger Dendritic Cell (gDC). This DC node is analogous to the HIS DCs as they are the first line of defense in HIS. The initiator gDC node sends a Route request to the nodes in the network. The nodes that already have a path to the destination will send back a Route Reply. Upon receipt of the Route Reply, the source gDC node calculates the Probability of communication nearness (P_{com}) [9] of those nodes from which a Route Reply was obtained. The packet is sent to the node that responded with the highest P_{com} value.

During this phase, the source node expects nodes to Acknowledge (ACK) packet receipt. In the case of a selfish node that does not send an ACK, a high priority PAMP signal is raised by the gDC node and the initiator node is also notified. The selfish node is forced to acknowledge receipt of high priority PAMP signal as this high priority packet overwrites the selfish node's buffer and there upon the packet signal will be transmitted as high priority by the previous gDC node.

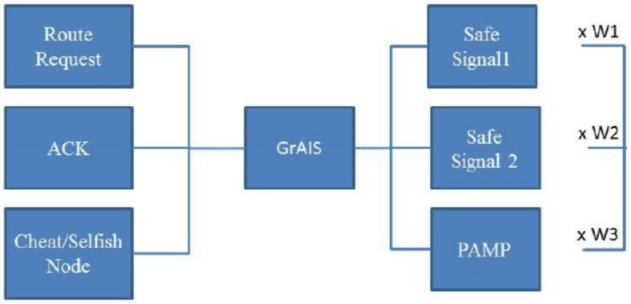

Figure 2: GrAIS model. The interaction types between nodes are shown along with the incorporation of the trust model in order to launch an immune response

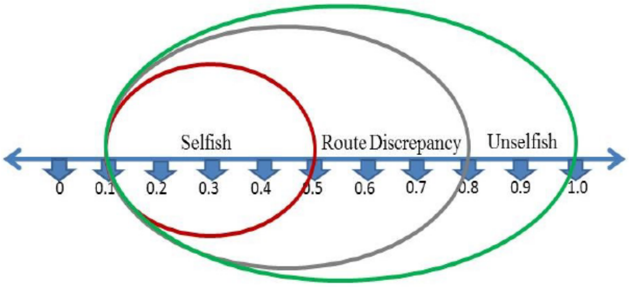

Figure 3: Trust number-line model

Similarly the gDC nodes, when they do not receive a response from the intermediate selfish node, inform the sender node and raises the high priority PAMP signal to validate the presence or absence of a selfish node. In our AIS based trust model, three trust signals are proposed:

- Safe Signal 1 (SS1) - This is generated upon receipt of Route Reply;
- Safe Signal 2 (SS2) - This is generated upon receipt of ACK;
- PAMP - This signal helps validate selfish node behavior. PAMP activates the immune response thereby protecting the host from infections in HIS. Similarly PAMP, being a high priority signal, overwrites the node buffer, and the selfish node will acknowledge receipt of the PAMP.

The trust value $T^{TP}_{a,,b}(t)$ is evaluated by *Node a* towards *Node b* at time t, TP is the trust purpose. $T^{TP}_{a,b}(t)$ is represented as a real number in the range [0, 1] as seen in Figure 3 where 1 indicates unselfish nodes, [0.5-0.8] indicates route error discrepancies and indicates a selfish behavior.

$$T^{TP}_{a,b}(t) = w_1 T^{SS1}_{a,b} + w_2 T^{SS2}_{a,b} + w_3 T^{PAMP}_{a,b} \qquad (1)$$

Where w_1, w_2, w_3, are the weights related to the trust components, with $w_1 + w_2 + w_3 = 1$.

Instead of assigning individual weights to each of the trust elements a priority signal, PAMP, is used and a signal, SAFE, to indicate the nodes are behaving correctly. The weight of the PAMP priority signal is shown by w_{PAMP}. The weight of the safe signal is shown by w_{SAFE}. Equation (1) can be rewritten as:

$$T_{a,b}(t) = w_{PAMP}[T^{PAMP}_{a,b}] + w_{SAFE}[T^{SS1}_{a,b} + T^{SS2}_{a,b}]. \qquad (2)$$

Where $w_{PAMP} + w_{SAFE} = 1$. A sliding window transmission approach is used to decrease the effect of conditions arising out of a network that could affect the trust calculation. We use a timing window (Δt) to determine the number of successful and unsuccessful packets sent between nodes. Let us consider a scenario where *Node a* evaluates *Node b* based on its behavior; thereby making *Node a* trustor and *Node b* the trustee. *Node c* sits beyond *Node b*. The trust relationship between nodes a, b and $c$as shown in Figure 4 is given by $(a, b) = (a, b) : (b, c)$.

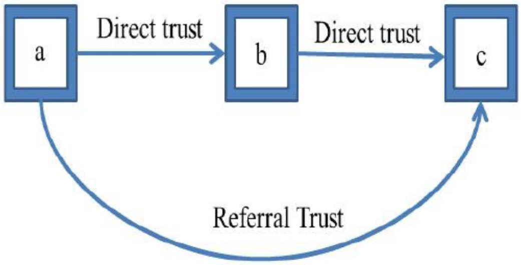

Figure 4: Trust relationship

Let the Trust Purpose be defined as "the node should be *good*." The trust between *Node a* and *Node b*will be direct therefore it's a functional (direct) level of trust whereas the trust between *Node a* and *Node c* will be indirect (referral) as well as an exponential decay factor of trust ρ is also considered therefore it's a referral level [13] of trust.

$$T^{TP}_{a,b,c}(t) = T^{TP}_{a,b}(t)P_{com} + T^{TP}_{b,c}(t)P_{com} + e^{-\rho\Delta t}T^{TP}_{a,c}P_{com}.$$

To compute$TRIALRESTRICTION$, we consider the number of interactions between nodes $a, b$and $c$over the maximum possible number of interactions that could occur with any neighbor node during the interval [*0, t*]. The hop count measure calculated by P$_{com}$ [9] and the Effective Energy of each node (EE_{node}) [10] is detrimental during the interaction between nodes in the GrAIS model. The flow chart of the GrAIS algorithm is as seen in Figure 5. In this approach, the following interaction categories, with regards to an unselfish node are considered, given that *Node a*:

- Sending Request;
- Receiving Reply;
- Selection of node based on highest value of P$_{com}$;
- Send Packet;
- If no ACK, send PAMP;
- If PAMP received, classify node as selfish node;
- gDC node will resend packet to selfish node.

P_{com} is an important factor while evaluating the trust purpose ($TRIALRESTRICTION$) between any two nodes as the packet will be sent to the node that responds with a route reply and highest P_{com} value. In this approach $TRIALRESTRICTION$ between any two neighboring nodes is computed by taking into account the number of communications between nodes $a$and $b$over the maximum possible number of interactions that could occur with any neighbor node during the interval [*0,t*]. The trust purpose for *Safe Signal 1* is computed by taking the ratio of the total number of route replies (N$_{RREP}$) received with the total number of route requests sent (N$_{RREQ}$). The trust purpose for *Safe Signal 2* is computed by taking the ratio of the total number of acknowledgment packets$TRIALRESTRICTION$ received by the sender with the route reply packets sent by the destination/intermediate ($TRIALRESTRICTION$ node. The trust purpose for the PAMP signal is computed by taking the ratio of the total number of PAMP sent for every route reply received by the sender and no acknowledgment sent by the destination/neighbor node.

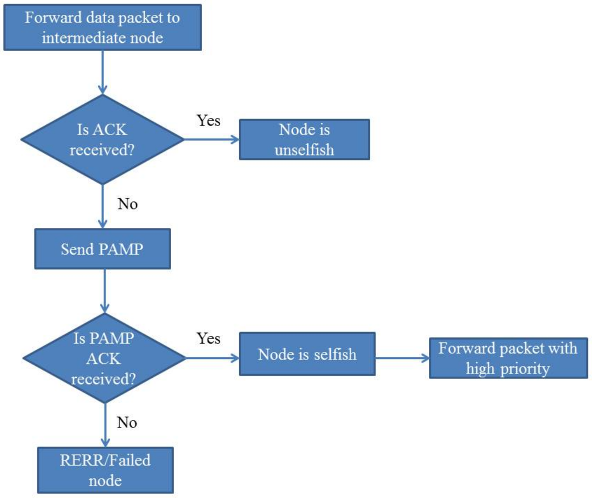

Figure 5: Flow of events in the proposed GrAIS model. The importance of PAMP signal is depicted in the flow chart.

$$\begin{aligned} T^{SS1}_{a,b}(t) &= [\frac{N_{RREP}}{N_{RQ}}]P_{com} \\ T^{SS2}_{a,b}(t) &= [\frac{N_{ACK}}{N_{RREP}}]P_{com} \\ T^{PAMP}_{a,b}(t) &= [\frac{N_{PAMP}}{N_{RREP}}]P_{com} \end{aligned}$$

The intermediate node informs the source node of a neighboring node that appears to be selfish. The source node sends a PAMP signal to overwrite the selfish node buffer and this selfish node is added to a blacklist to prevent it being used in future communications if it does not respond to the PAMP signal. The high priority PAMP signal plays a vital role in this process. The "Activate DC" mode that is switched on due to a selfish node being identified sets in motion the response process. The effect of the PAMP signal in the presence of selfish nodes and its impact on packet loss ratio can be seen in Figure 6. As the PAMP effect to deal with the selfish nodes, the packet loss ratio is reduced.

The source node sends a PAMP signal, $PAMP_{send}$ and each node have to acknowledge receipt by sending back a PAMP receive signal, $PAMP_{recv}$. The selfish node that did not formerly acknowledge receipt of the packet will be forced to respond with a PAMP receive signal, $PAMP_{recv}$, as the PAMP signal is a high priority message and it overwrites the node buffer.

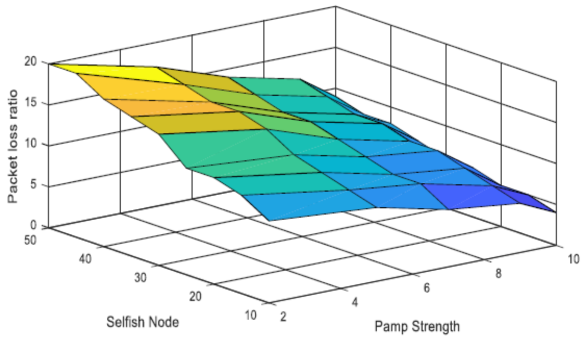

Figure 6: Weight of PAMP signal strength

Once *Node a* obtains $T_{a,b}^{TP}$ for $TP = Safe$ Signal1, Safe Signal 2 and PAMP then $T_{a.b}^{TP}$ is calculated based on Equation (2).

- $T_{a,b}^{SS1}(t)$: Measures the number of times any intermediate (trustee) node generated a route reply. Here a settlor node evaluates the unselfish and honest behavior of the trustee node. This trust component is computed based on the number of interactions between the trustor and trustee node.

- $T_{a,b}^{SS2}(t)$: The trust element is evaluated when the trustee node sends back an acknowledgment of receipt of a packet.

- $T_{a,b}^{PAMP}(t)$: Analysed by observing if the intermediate node received no acknowledgment to the data packet but it did send a route reply earlier, and then the PAMP signal is sent to validate selfish behavior in a node.

The GrAIS utilizes the concept of a Price of Anarchy [9] for load calculation. Consider there are N nodes in the network. In the GrAIS model, nodes that perform routing task employ a trust purpose $T_{a,b}^{TP}$ between any two nodes a, b. The Effective Energy of the *Node b* and Trust value of *Node b* as observed by *Node a*is taken into consideration. Therefore, the Workload *(WL)* in a routing task undertaken by any *Node b* is

$$WL_b = \frac{1}{EE_{node(b)} T_{a,b}^{TP}(t)} \tag{3}$$

The workload is dependent on the energy of a node or inversely proportional to node energy and trust. Equation (3) shows that as workload increases the nodes expend more energy to carry out networking tasks. As the node energy consumption increases the trust value could reduce.

5 Simulation Results and Analysis

The simulations were carried out using NS-3 and MATLAB. Energy-aware workload [12] distribution is the most efficient approach to reduce energy consumption and stimulate cooperation of selfish nodes. In the traditional applications of MANETs, the workloads are very simple and wireless communication is usually the most energy-intensive process. However, as the applications of MANETs become more complex, it becomes necessary to efficiently distribute the workloads by considering both the trust, hop count and communication energy consumption. In this paper, we consider workload in terms of the trust metric and energy consumption during packet transmission. The workload in terms of packet transmission is considered to reveal the tradeoff between sucker (good) nodes and selfish (cheat) nodes. In our simulations, there are three workload scenarios explored with the packet delivery workload increasing from Workload-1 to Workload-3.

Table 1: Simulated parameters

Simulator	Ns-3.23
Mobility Model	Random waypoint
Simulation Time	1000s
Number of selfish nodes	10-50
Number of nodes	150
Traffic Type UDP Network Area	300m*1500m
Packet size	130 bytes
Mobility	20 m/s
Transmission Range	50m

In Figure 7 and Figure 8, it can be observed that initially good nodes maintain trust while the selfish nodes choose to conserve their energy. As the workload is initially light and all nodes have more energy, the unselfish characteristic amongst participating nodes becomes a crucial factor when determining trust. The prominent drop in trust amongst the good nodes was observed at $t = 300$ min when the good nodes had depleted their energy to a point where they began to look for alternative pathways that would conserve the energy of known good nodes. The GrAis model performs better as time progresses due to selfish nodes being forced to co-operate. The selfish node maintains trust for a longer t as it would have conserved energy to this point.

In Figure 8, the trend is similar to Figure 7, except that the time during which good nodes start to show a dip in trust occurs earlier than when it occurred in the GrAIS model. This is due to the increase from Workload-1 to Workload-2. As workload increases the energy consumption would also increase and good nodes would diminish their energy store at a corresponding rate whilst cheat nodes act to retain energy. The GrAIS model facilitates traffic flows using selfish nodes and as a result the GrAIS model is able to function more effectively as time progresses when compared to a model that relies upon good nodes to transfer traffic flows. In Figure 9, a new trend is seen with the cheat nodes acting to conserve energy

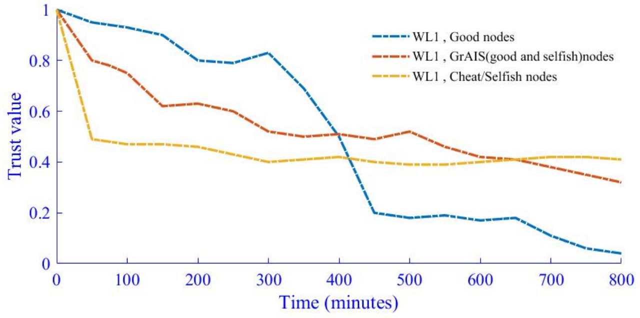

Figure 7: Trust values plotted against time under Workload-1

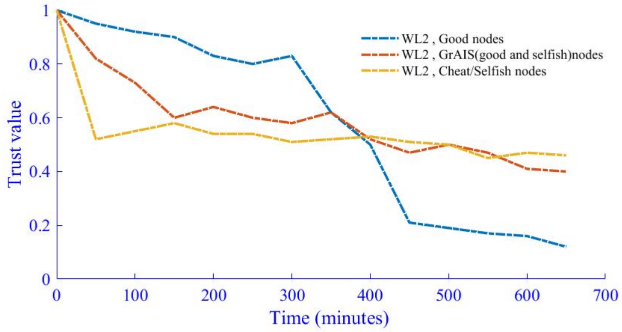

Figure 8: Trust values plotted against time under Workload-2

earlier due to the higher workload and this results in a lack of cooperation from the point where trust dips. The GrAIS model approaches the good node model by forcing the selfish nodes to cooperate with the help of the high priority PAMP signal.

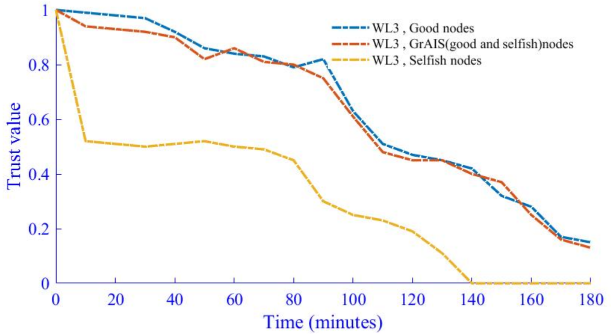

Figure 9: Trust values plotted against time under Workload-3

Using a Packet Delivery Ratio (PDR) metric, as shown in Figure 10, we can evaluate the performance of the proposed GrAIS algorithm. The PDR is a performance metric used in MANET to evaluate the performance of a routing protocol. It is the ratio of the number of data packets delivered to the number of packets sent. GrAIS shows an improved packet delivery ratio while SAODV [14] exhibits a decrease in packet delivery ratio as the number of selfish nodes increases while CITA-AODV [15] follows closely behind GrAIS.

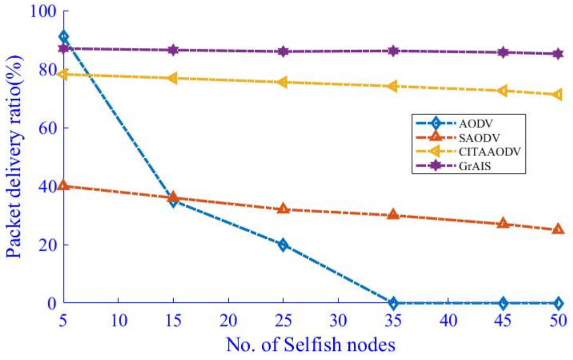

Figure 10: Packet delivery ratio v/s number of selfish nodes

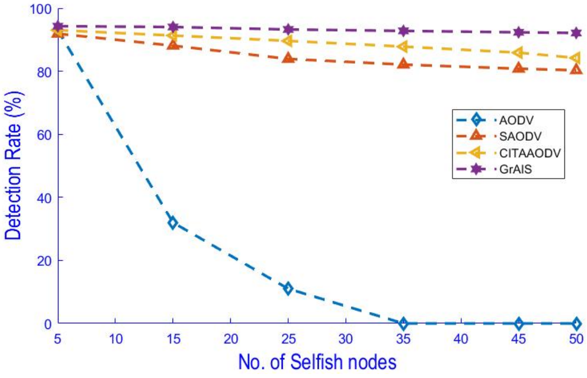

Figure 11: Detection ratio v/s number of selfish nodes

The detection rate has been compared against the number of selfish nodes in the network. A detection rate of 93.41% was achieved while for SAODV the detection rate achieved was 85.34%. This shows that as the number of selfish nodes increases, GrAIS is able to detect the selfish nodes due to its better trust framework.

6 Conclusion and Future Work

The GrAIS model approach presented in this paper shows that selfish nodes need not be identified and isolated as there should be an opportunity to force the selfish nodes to participate using high priority signals thereby spreading the load and resource utilization. It is important for network survivability and successful task completion that all MANET nodes cooperate and participate. In some scenarios, it is deemed necessary to include selfish nodes by forcing them to cooperate instead of overlooking their selfish behavior or isolating them from the MANET, as this would reduce the opportunity to leverage this resource. The GrAIS model utilizes the principles of AIS and probability to create a model incorporating good and selfish nodes to combat selfishness in MANET. The results obtained from the simulations have shown that the GrAIS model outcomes are an improvement over models that ignore or isolate selfish nodes as time progresses in spite of increasing workload. A balance between energy utilization, due to good nodes transferring traffic, and energy conservation, due to selfish nodes refusing to transfer traffic, has been achieved by forcing selfish nodes to participate at an appropriate point in the MANET life cycle. A MANET that combines selfishness and unselfishness can be shown to be beneficial when resources, particularly energy, become limited. As future work, a more complex model could be developed exclusively for higher workloads by considering the stability of the GrAIS model over a longer time interval.

References

[1] C. Perkins, E. Belding-Royer, and S. Das, *Ad hoc On-Demand Distance Vector (AODV) Routing*, RFC, 2003.

[2] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, pp. 255-265, 2000.

[3] Y. Yoo and D. P. Agrawal, "Why does it pay to be selfish in a MANET?," *IEEE Wireless Communications*, vol. 13, pp. 87-97, 2006.

[4] D. G. Kampitaki, E. D. Karapistoli, and A. A. Economides, "Evaluating selfishness impact on MANETs," in *International Conference on Telecommunications and Multimedia (TEMU'14)*, pp. 64-68, 2014.

[5] S. Buchegger and J. Y. Le Boudec, "Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks," in *10th Euromicro Workshop on Parallel, Distributed and Network-based Processing*, pp. 403-410, 2002.

[6] S. Gupta, C. Nagpal, and C. Singla, "Impact of selfish node concentration in MANETs," *International Journal of Wireless & Mobile Networks*, vol. 3, pp. 29-37, 2011.

[7] M. T. Tran and V. Simon, "Can altruism spare energy in ad hoc networking?" in *Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia*, pp. 214-217, 2011.

[8] L. E. Jim and M. A. Gregory, "State analysis of Mobile Ad Hoc Network nodes," in *International Conference on Telecommunication Networks and Applications Conference*, pp. 314-319, 2015.

[9] L. E. Jim and M. A. Gregory, "Packet Storage Time attack-a novel routing attack in Mobile Ad hoc Networks," in *26th International Conference on Telecommunication Networks and Applications Conference*, pp. 127-132, 2016.

[10] R. Dawkins, *The Selfish Gene*, New York: Oxford, 2006.

[11] W. Yu, Y. Huang, and A. Garcia-Ortiz, "Modelling optimal dynamic scheduling for energy-aware workload distribution in wireless sensor networks," in *International Conference on Distributed Computing in Sensor Systems*, pp. 116-118, 2016.

[12] Jøsang, A. and S. Pope, "Semantic constraints for trust transitivity," *Proceedings of the 2nd Asia-Pacific Conference on Conceptual Modelling,* vol. 43, pp. 59-68, 2005.

[13] D. Cerri and A. Ghioni, "Securing AODV: the A-SAODV secure routing prototype," *IEEE Communications,* vol. 46, no. 2, 2008.

[14] A. Khannous, A. Rghioui, F. Elouaai, and M. Bouhorma, "Securing MANETS using the integration of concepts from diverse immune theories," *Journal of Theoretical and Applied Information Technology*, vol. 88, pp. 35, 2016.

[15] K. D. Elgert, *Immunology: Understanding the Immune System*, John Wiley & Sons, 2009.

[16] M. Abdelhaq, R. Hassan, M. Ismail, R. Alsaqour, D. Israf, "Detecting sleep deprivation attack over MANET using a danger theory-based algorithm," *International Journal on New Computer Architectures and Their Applications*, vol. 1, pp. 534-541, 2011.

[17] S. Forrest, A. S. Perelson, L. Allen, R. Cherukuri, "Self-non self discrimination in a computer," *IEEE Symposium on Research in Security and Privacy,* pp. 202-212, 1994.

[18] J. Timmis, M. Neal, J. Hunt, "An artificial immune system for data analysis," *Biosystems,* vol. 55, pp. 143-150, 2000.

[19] A. O. Tarakanov, V. A. Skormin, S. P. Sokolova, *Immunocomputing: Principles and Applications*, Springer, New York, 2003.

[20] R. Steinman and Z. Cohn, "Identification of a novel cell type in peripheral lymphoid organs mice," *The Journal of Experimental Medicine*, vol. 137, no. 5, pp. 1142-1162, 1973.

[21] M. L. Kapsenberg, "Dendritic-cell control of pathogen-driven T-cell polarization," *Nature Reviews Immunology*, vol. 3, pp. 984-993, 2003.

[22] T. Jamie and U. Aickelin, "Towards a conceptual framework for innate immunity," in *3rd International Conference on Artificial Immune Systems*, pp. 112-125, 2004.

[23] J. Greensmith and U. Aickelin, "The deterministic dendritic cell algorithm," in *7th International Conference on Artificial Immune Systems*, pp. 291-302, 2008.

[24] J. Greensmith, U. Aickelin, J. Twycross, "Articulation and clarification of the dendritic cell algorithm," in *5th International Conference on Artificial Immune Systems*, pp. 404-417, 2006.

[25] J. Twycross and U. Aickelin, "Libtissue-implementing innate immunity," in *IEEE Congress on Evolutionary Computation*, pp. 499-506, 2006.

[26] P. Matzinger, "The danger model: A renewed sense of self," *Science*, vol. 296, no. 5566, pp. 301-305, 2002.

[27] P. Bretscher and M. Cohn, "A theory of self-non self discrimination," *Science*, vol. 169, pp. 1042-1049, 1970.

[28] U. Aickelin and S. Cayzer, "The danger theory and its application to artificial immune systems," in *1st International Conference on Artificial Immune Systems (ICARIS'02)*, pp. 141-148, 2002.

[29] P. K. Suri and K. Taneja, "Exploring selfish trends of malicious mobile devices in MANET," arXiv preprint arXiv: 1005.5130, 2010.

Biography

Lincy Elizebeth Jim received a PhD from School of Engineering RMIT University, Melbourne, Australia in 2017; she is a recipient of the Student Travel Award-ITNAC 2016. She has also received the Juniper Networks Certified Associate (JNCIA-Junos) certification. She has more than 5 years of working experience as an Oracle Technical Analyst. She received her Master degree in Electronics and Communication Engineering from National Institute of Technology, Calicut, India in 2007 and her Bachelor of Electronics and Communication Engineering from Cochin University of Science and Technology in 2003.

Mark A Gregory (SM'99) is a Fellow of the Institute of Engineers Australia and a Senior Member of the IEEE. Mark A Gregory received a PhD from RMIT University, Melbourne, Australia in 2008, where he is an Associate Professor in the School of Engineering. In 2009, he received an Australian Learning and Teaching Council Citation for an outstanding contribution to teaching and learning. He is the Managing Editor of two international journals (AJTDE and IJICTA) and the General Co-Chair of ITNAC. Research interests include telecommunications, network design and technical risk.