Malicious Node Elimination Using Fine Grained Analysis A Trust Based Scheme In MANET

K.L.Subhasree[1], Dr.S.Sargunavathi[2]
[1]Dept of Applied Electronics
[2]Associate professor, Dept of Applied Electronics
[1, 2] Sriram Engineering College, Perumalpattu

Abstract- *Mobile Ad Hoc network (MANET) is a self-configured and infrastructure less network that consists of mobile nodes. Due to decentralized nature and dynamic topology, the packet loss occurs by malicious nodes. Malicious node is node seeking to deny the service to other nodes and modifies the data before, during or after transmission in the network. There are several other causes for packet loss such as interference, queue overflow and node mobility. Hence packet loss is a crucial issue in MANET. To sort out this issue, a light weight packet drop detection (LiPaD) for Ad Hoc networks is used. It suggests that every node must keep a count of received/forwarded packets and periodically report to a coordinator node for analysis and malicious node detection. Such technique considers each packet loss as misbehavior by malicious nodes, without analyzing the other possible causes of packet losses. To solve this issue, this project presents a fine grained analysis with special queue (FGA) which examines the cause for packet loss and inform the reason for the loss. The objective of the project is to identify the malicious nodes using network factors such as MAC layer information, node mobility and queue overflow to determine the packet losses. By this the malicious nodes is detected and eliminated, also the network security is ensured. The FGA algorithm is simulated in network simulator (NS2). FGA-S scheme is evaluated in terms of effectiveness under network parameters such as throughput ratio, packet delivery ratio, energy level routing overhead and average end to end delay. The inventive results show that the proposed trust model achieves a significant reduction in false positive rate and an increase in the rate of detection of malicious nodes.*

Keywords- MANET, malicious nodes, trust, security, fine grained analysis.

I. INTRODUCTION

Mobile Ad-hoc Networks (MANET) comprises a collection of mobile nodes which are interconnected to one another through wireless connections in an infrastructure less network. Though cooperative operation is required by every node for ensuring effective functioning of the MANET, several limitations like rapidly modifying topology and non-centralized architecture, they are susceptible to diverse attacks through misbehaving nodes. For instance, a node will drop the data packet because of malicious actions, node offers wrong path to neighboring nodes in which the data may be wrongly send or never sent to the target, and also affects the efficiency. The detection and segregation for such disobedient nodes in MANET is necessary, so many trust-based security models have been drawn up. Here, trust can be represented as the level of fulfilling the expectation of other nodes. Under trust based models, every node in the network will manage an independent trust table for computing and storing the trust values. Utilizing the computed trust value, Routing decisions were made. In some instances, the existing trust based models failed to identify the exact reasons of malicious occurrence. It results to various false positives where the genuine nodes are considered as malicious. This problem occurrence took place in those trust based security model because it considers that the packet loss happens only by the malicious nodes. On the other hand, packets will be lost in MANET because of several actions like wireless link transmission error, mobility and congestion. Without a proper analysis false rate increases under highly mobile and high data rate conditions. This paper presents a Fine grained analysis with special queue (FGA) model which examines the cause for packet loss and inform reason for loss.

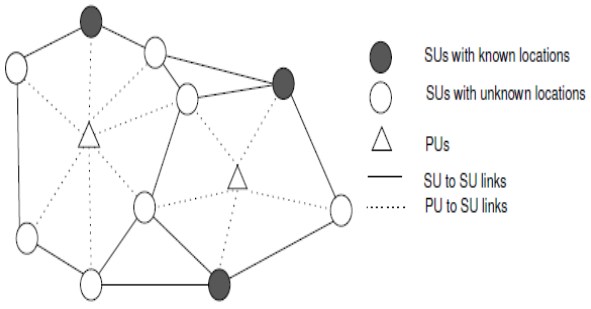


Figure. Sample network

II. LITERATURE SURVEY

It can be broadly classified into three categories. The initial category includes algorithms that consider the reliability of links to find more reliable routes. For instance, De Couto et al. [1] introduced the notion of expected transmission count

(ETX) to find reliable routes that consist of links requiring less number of retransmissions for lost packet recovery. In spite of less energy consumption for less retransmission they essentially do not minimize the E2E packet traversal. Furthermore, considering a higher priority for reliability of routes may result in overusing some nodes. If there are some links more definitive than others, then these links will customarily be used to forward packets. Nodes along these link will then fail quickly, since they have to forward many packets on behalf of other nodes. The second category includes algorithms that aim at finding energy-efficient routes (e.g., the proposed algorithms in [2], [3], [4], [5], [6], [7]). These algorithms do not consider the remaining battery energy of nodes to avoid overuse of nodes, even though some of them, namely, [4], [5], [6], [7], address energy-efficiency and reliability together. Apart from this, many routing algorithms—including energy efficient algorithms proposed in [2], [3], [4], [5], [6], [7]—have a major drawback. Observation of the real consumed energy of nodes to discover the energy efficient routes is not considered. They only consider the transmission power of nodes (the output power of the power amplifier) neglecting the energy consumed by processing elements of transmitters and receivers. What is considered as energy cost of a path by these algorithms is only a fraction of the actual energy cost of nodes for transmission along a path. As we will show, this negatively affects energy- efficiency, reliability, and the operational lifetime of the network altogether. The last category includes algorithms that try to prolong the network lifetime by finding routes consisting of nodes with a higher level of battery energy .These algorithms, however, do not label the other two characteristics, i.e., reliability and energy-efficiency. The located routes by these algorithms may neither be energy-efficient nor be reliable. This can increase the overall energy consumption in the network. Thus, the network life time may even be reduced.

Our in-depth work in this paper considers energy efficiency, reliability, and prolonging the network lifetime in wireless ad hoc networks holistically. We propose a novel energy-aware routing algorithm, called reliable minimum. Energy cost routing (RMECR). RMECR finds energy efficient and reliable routes that increase the operational lifetime of the network. In the design of RMECR, we use an in-depth and detailed analytical model of the energy Consumption of nodes. RMECR is proposed for networks with hop-by-hop (HBH) retransmissions providing link layer reliability, and networks with E2E retransmissions providing E2E reliability. HBH retransmission is supported by the medium access control (MAC) layer (more precisely the data link layer) to increase reliability of packet transmission over wireless links. Nevertheless, some MAC protocols such as CSMA and MACA may not support HBH retransmissions. In such a case, E2E retransmission could be used to ensure E2E reliability [4], [5], [16]. Our work has also some important and novel ideas compared to the pioneering studies like [2], [3], [4], [5], [6], [7], which also address the problem of energy-efficient reliable routing in wireless ad hoc networks. 1) We consider the impact of limited number of transmission attempts on the energy cost of routes in HBH systems. This effect has been neglected in [4], [5] and have not been addressed in depth in [6], [7]. We show that by taking this limitation into account, a shortest-path routing algorithm like Dijkstra's algorithm—which has been considered as an optimum solution in [2], [3], [4], [5], [6], [7] for the problem of minimum energy routing in wireless ad hoc networks— does not provide an optimal solution. It is a heuristic solution, and it can be an optimal solution only if the number of retransmissions on each link is large enough to ensure complete reliability of links. 2) We consider the impact of acknowledgment packets on energy cost of routes in both HBH and E2E systems. This impact has been neglected in [2], [3], [4], [5], [6], [7]. By considering this, we show that in the E2E systems, the energy cost of packet transmission from a source node to an intermediate node depends on both upstream and downstream links of that intermediate node, neglecting the impact of acknowledgement packets means that we disregard the impact of downstream links on the energy cost. 3) We consider energy consumption of processing elements of transceivers. As mentioned earlier, underestimating the energy consumption of transceivers can severely harm reliability and energy efficiency of routes. A detailed consideration toward various aspects of the energy consumption of nodes makes our work realistic and thus closer to practical implementations.

III. EXISTING SYSTEM

High malicious dropping rates is the first category aims at high malicious dropping rates, where most (or all) lost packets are caused by malicious dropping. In this case, the impact of link errors is ignored. Most related work falls into this category. Based on the methodology used to identify the attacking nodes, these works can be further classified into four subcategories. O Credit systems A credit system provides an incentive for cooperation. A node receives credit by relaying packets for others, and uses its credit to send its own packets. As a result, a maliciously node that continuous to drop packets will eventually deplete its credit, and will not be able to send its own traffic. O Reputation systems A reputation system relies on neighbors to monitor and identify misbehaving nodes.

A node with a high packet dropping rate is given a bad reputation by its neighbors. This reputation information is propagated periodically throughout the network and is used as

an important metric in selecting routes. Consequently, a malicious node will be excluded from any route. O End-to end or hop-to-hop acknowledgements to directly locate the hops where packets are lost. A hop of high packet loss rate will be excluded from the route. O Cryptographic methods Bloom filters used to construct proofs for the forwarding of packets at each node. By examining the relayed packets at successive hops along a route, one can identify suspicious hops that exhibit high packet loss rates. Number of maliciously dropped packets is significantly higher than that caused by link errors the second category targets the scenario where the number of maliciously dropped packets is significantly higher than that caused by link errors, but the impact of link errors is non-negligible.

IV. PROPOSED SYSTEM

Fundamental Concept

In this section, we set up the fundamental boundaries to use in summing up the connections between nodes reliant on the assessment of bundle misfortune. For separation among a packet drop either on account of network status or assaults by malicious nodes, a bunch of boundaries are examined to search for the genuine explanation of bundle misfortune. Each boundary lies in the worth scopes of 0 to 1. Additionally, it is noticed that the FGA model is put at each node present in the network.

A. MAC LAYER INFORMATION

A packet may be lost at the MAC layer of a sending node for a few causes specifically out-of-range next hop or out of date routing gets to. Consequently, the MAC layer information is considered as one of the mostly fundamental boundaries to assess the plausible reasons of packet disappointment between 2 nodes. As pronounced in the IEEE 802.11 MAC layer prerequisites, a dispatcher node sends a data packet and gets link layer acknowledgment from the beneficiary. To examine a link for likely correspondence of data packet, [13] introduced an interaction of sending a hunt packet past to sending the genuine data packet. Every node communicates tests at a normal period t.

Each node recalls the tests it gets during the last w seconds. At the point when nodes are getting likely number of SHAREIT interchanges from neighbor nodes, it implies that there are no meddling links over the link. In this way, when a node drops a data packet, it very well may be perceived as a wicked node, killing the chance of a link issue. In any case, when a node doesn't get the anticipated number of SHAREIT correspondences from different neighbor nodes, it is viewed as that few link meddling issues exists among these two nodes. A node A can compute the likelihood that the data packet would be adequately sent to a node B with checking the estimation of the link layer among the two nodes by the utilization of SHAREIT packets. The ensuing recipe is used for registering the packet forwarding probability at the MAC layer among 2 nodes:

$$P_M = \frac{\xi_{recv(t_{i-1},t_i)}}{\xi_{exp(t_{i-1},t_i)}}$$

Where $\xi_{recv}$is the total number of SHAREIT packets received and $\xi_{exp}$is the expected number of SHAREIT packets during a particular interval (t_{i-1}, t_i).

B. QUEUE OVERFLOW

In MANETs, queue can be flooded as a result of numerous simultaneous jobs in particular being together switches and terminals with multi jump forwarding nodes, and to the regular correspondence of geography messages. In the event that the measure of routing traffic is amazingly high, data traffic may not communicate at all or being sent at a minuscule rate that may prompts stagnation. Due to queue flood in a node, packet could be lost with a forwarding node, and this node may be unmistakable as malicious with the source node despite the fact that it isn't. Besides, blockage resultant from a measure of data packets which surpasses the queue length may likewise brings about packet misfortune by queue flood. Traffic load intensity (TLI) [14] is the measurement use to choose the queue position at the closest nodes. Here, a source node remains track of the latest traffic load information at each forwarding node in a table. Each forwarding node now and again models its limit queue length in the MAC layer, and relates to the source node as a division of its SHAREIT correspondences. Let B exist a forwarding node, let q exist the y test esteem indicating the queue length at the current second, and Q be the queue length test tally assembled over the term of interest, and the normal load traffic at node B could be characterized by

$$P \quad = 1 - TLI$$

The packet forwarding prospects are associated with the TLI that implies a lesser estimation of the TLI prompts a high packet forwarding probability and the other way around. It is alluring to specify that a high node thickness (indication an enormous number of neighbor nodes) as a rule prompts additional traffic and high TLI to forwarding nodes, in this

manner, lessens the general packet forwarding plausibility. It is fundamental to accept the security plans if a malicious node doesn't straightforwardly go behind the convention and stays in its queue position. For instance, a malicious node may characterize that the queues are consistently full. Such a node will be wiped out from the routing pathway, an undesirable outcome to assailants. Thusly, malicious node has little reason to disperse wrong status data concerned the queue, as nodes through potential queue flood would not be picked as forwarding nodes.

C. MOBILITY

Primarily the trust subordinate frameworks influence listening in strategies to assess the trust estimations of the node. In such techniques, a node which advances a packet to its ensuing jump likewise tune in the re-correspondence of the packet to the resulting bounce in the indiscriminate mode. It is vital in make certain, eventually, a precise salvage of the packet to its completion target. At the point when source nodes tune in the packet forwarding from the forwarding node, it is estimated as a fruitful correspondence; or disaster will be imminent, it is estimated as underhandedness. Under certain cases, when a source node couldn't accurately catch the re-correspondence of its packet in spite of the fact that it occurred, or an objective node are difficult to reach due to old routing information, a generously forwarding node may be observable as making trouble. For this reason, node versatility has a fundamental part in seeing the duty of a forwarding node. A node could set up the versatility of the nodes in its close by zone by assessing the close by pace of link changes. Such rate could be utilized to inspect the likely reasons of packet disappointment activities. The pace of link adjustments at node *z* can be characterized with the resulting condition:

$$\eta = \lambda + \mu$$

the chance of effective packet forwarding through rate of link alterations could be made as:

$$P = 1 - \eta$$

It is perceptible from the greatest paces of link adjustments indicate additional unique neighborhood which prompts a lesser chance of effective packet forwarding. Utilizing the combination of packet misfortune prospects, a last packet forwarding likelihood record (FPI) [10] can be characterized. It demonstrates the chance wherein a packet can be appropriately sent.

$$FPI_A^B = \frac{\alpha P_M + \beta P_Q + \gamma P_\eta}{\alpha + \beta + \gamma}$$
$$where\ \alpha + \beta + \gamma = 1$$

Where,
α, β, and *γ* are the weights assigned to each one of the parameters

The estimation of the FPI will be determined by a source node and contrasted with the current conduct of every node, to rate the rightness of the registered reliability level by the fundamental trust-based plan.

D. FGA model

The FPI of each neighbor node can be dictated by a source node .It is contrasted with the current activity of each node, to assess the rightness of the determined trust level by applying the trust based model.

Procedure FGA
For all neighbor node v do

If FPI < FPI_A^B then
The node is malicious
Eliminate that node
proceed
If FPI > FPI_A^B then
Packet loss is due to three factors
Find the exact factor
eliminate it
proceed
End if
End for
End FGA

V. RESULT ANAYSIS

In this section, we evaluate the effectiveness of our FGA scheme. Network Simulator 2 (NS-2) [36] version 2.34 is used to implement and analyze the performance of the scheme.

SIMULATION PARAMETERS

TABLE 1

Simulation time	1000 seconds
Number of nodes	60
Number of malicious nodes	3-18
Network size	1000m × 1000m
Transmission range	250m
Simulation speed	1m/s- 10m/s
Mobility model	Random way point
Traffic type	Constant Bit Rate (CBR)
IFQ size	50 (NS-2 default)
Channel bandwidth	2 Mbps

a. PACKET DELIVERY RATIO:

The delivery rate analysis of the proposed method under varying number of attacker nodes. From the figure, it can be seen that the presented model attains maximum delivery ratio over the compared methods. With increasing attacker node density, the number of data connections in the network also increases; hence more packets are dropped in the network due to collisions. The existing schemes consider normal packet drops as misbehaving activity from legitimate nodes. Therefore, the delivery ratio is again higher in the presented FGA scheme than other methods. The presented FGA model offered maximum delivery with the 6% than existing system.

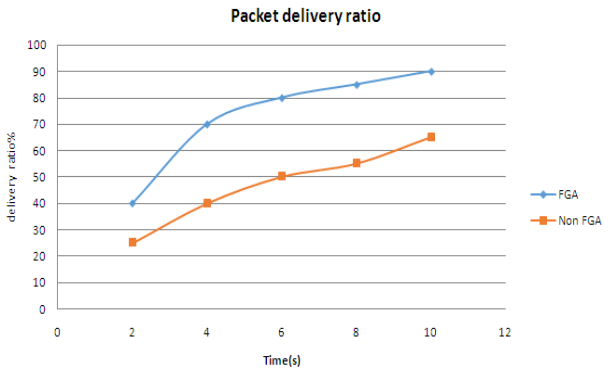


Figure (a) Packet delivery ratio Vs Time

b. THROUGHPUT:

The results attained by different techniques interns of throughput. By looking into the figure, it is evident that the Non FGA exhibits less performance by attaining least throughput value. The presented FGA technique showed maximum performance with highest value of throughput. For instance, under the presence of minimum 5 nodes, the Non FGA fails to show case effective results and achieved a minimum throughput of 49.3kbps. Subsequently, the Non FGA model manages well and offered high throughput of 52.3kbps. However, the projected FGA model outperforms these two methods by attaining maximum throughput of 55.8kbps.The figure indicates that the throughput is decreased with the increase in the node count.

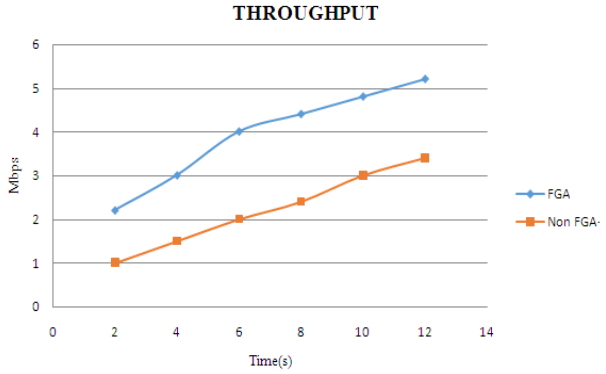
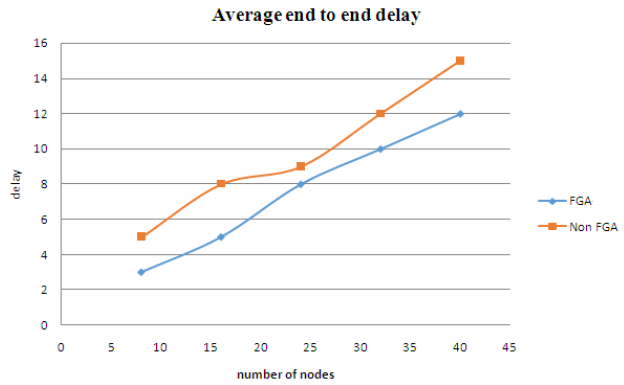


Figure (b) Throughput Vs Time

c. AVERAGE END TO END DELAY:

The investigation of the result are obtained by the paper and compared methods in terms of delay. The technique which incurs less delay indicates better performance. In this figure, the projected FGA model shows effective outcome with minimum delay whereas the compared Non FGA leads to high delay.



Figure(c) Average end to end delay Vs Number of nodes

d. ENERGY EFFICIENCY:

For instance, under the presence of minimum 5 nodes, the Non FGA fails to showcase effective results and achieved a maximum energy utilization of 7.1J. FGA model outperforms thIS methods by attaining minimum energy consumption of 1.5J. From these values, it is also noticed that the energy utilization gets drastically increased with increasing node count.

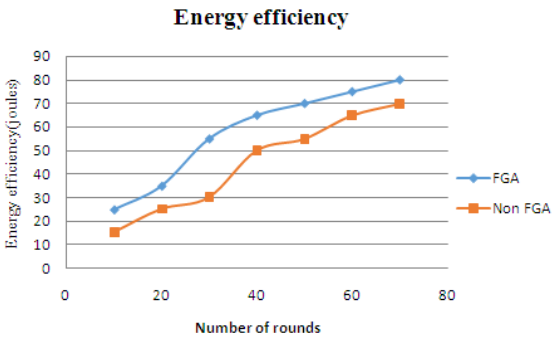


Figure (d) Energy efficiency Vs Number of rounds

e. ROUTING OVERHEAD:

For instance, under the presence of minimum 5 nodes, the Non FGA fails to showcase effective results and achieved a maximum overhead of 6.9%.The FGA model outperforms the method by attaining minimum overhead of 1.5%.

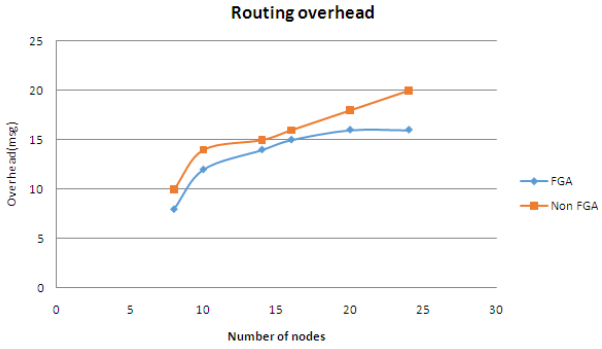


Figure (e) Routing overhead Vs Number of nodes

VI. CONCLUSION

Link errors and malicious drop is identified. In the insider-attack case, whereby malicious nodes that are part of the route exploit their knowledge of the communication context to selectively drop a small amount of packets critical to the network performance. Because the packet dropping rate in this case is comparable to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy. To improve the detection accuracy, the correlations between lost packets is identified. Homomorphic linear authenticator (HLA) based public auditing architecture is developed that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This construction is privacy preserving, collusion proof, and incurs low communication and storage overheads. To reduce the computation overhead of the baseline scheme, a packet-block based mechanism is also proposed, which allows one to trade detection accuracy for lower computation complexity. The implementation of this FGA scheme under other routing protocols and analysis of other performance metrics would be done in future.

REFERENCES

[1] D.S.J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A High Throughput Path Metric for Multi-Hop Wireless Routing," Proc. ACM MobiCom, pp. 134-146, 2003.

[2] S. Singh and C. Raghavendra, "PAMAS—Power Aware Multi Access Protocol with Signalling for Ad Hoc Networks," ACM Computer Comm. Rev., vol. 28, pp. 5-26, 1999.

[3] J. Gomez, A.T. Campbell, M. Naghshineh, and C. Bisdikian, "PARO: Supporting Dynamic Power Controlled Routing in Wireless Ad Hoc Networks," Wireless Networks, vol. 9, no. 5, pp. 443-460, 2003.

[4] S. Banerjee and A. Misra, "Minimum Energy Paths for Reliable Communication in Multi-Hop Wireless Networks," Proc. ACM MobiHoc, pp. 146-156, June 2002.

[5] Q. Dong, S. Banerjee, M. Adler, and A. Misra, "Minimum Energy Reliable Paths Using Unreliable Wireless Links," Proc. ACM MobiHoc, pp. 449-459, May 2005.

[6] X.-Y. Li, Y. Wang, H. Chen, X. Chu, Y. Wu, and Y. Qi, "Reliable and Energy-Efficient Routing for Static Wireless Ad Hoc Networks with Unreliable Links," IEEE Trans. Parallel and Distributed Systems, vol. 20, no. 10, pp. 1408-1421, Oct. 2009.

[7] X. Li, H. Chen, Y. Shu, X. Chu, and Y.-W. Wu, "Energy Efficient Routing with Unreliable Links in Wireless Networks," Proc. IEEE Int'l Conf. Mobile Adhoc and Sensor Systems (MASS '06), pp. 160-169,2006.

[8] S. Singh, M. Woo, and C.S. Raghavendra, "Power-Aware Routing in Mobile Ad Hoc Networks," Proc. ACM MobiCom, Oct. 1998.

[9] C. Toh, "Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad Hoc Networks," IEEE Comm. Magazine, vol. 39, no. 6, pp. 138-147, June 2001.

[10] D. Kim, J.J.G. Luna Aceves, K. Obraczka, J. Carlos Cano, and P. Manzoni, "Routing Mechanisms for Mobile Ad Hoc Networks Based on the Energy Drain Rate," IEEE Trans. Mobile Computing, vol. 2, no. 2, pp. 161-173, Apr.-June 2003.

[11] J.-H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol. 12, no. 4, pp. 609-619, Aug. 2004.

[12] A. Nagy, A. El-Kadi, and M. Mikhail, "Swarm Congestion and Power Aware Routing Protocol for

Manets," Proc. Sixth Ann. Comm. Networks and Services Research Conf., May 2008.