Wireless Ad-hoc Networks: Employing Behaviour History to Combat Malicious Nodes

H. Hallani
School of Computing and Mathematics
University of Western Sydney, *Australia*
hhallani@scm.uws.edu.au

S. A. Shahrestani
School of Computing and Mathematics
University of Western Sydney, *Australia*
seyed @computer.org

Abstract—**The presence of malicious nodes in Ad-hoc networks, which operate without a central administration infrastructure, can result in performance degradation or even disruption of the network operation. This paper investigates this topic further and proposes some approaches to mitigate the consequences of the presence of the malicious nodes in Ad-hoc networks. Experimental and simulation results that show the effect of such nodes on the performance of the network are reported and analyzed. To achieve higher levels of security and reliability, an approach that is based on the utilization of past behaviour of all member nodes is investigated and reported. The main goal for this approach is to identify routes between the source and the destination, which excludes and if not possible, minimizes the number of malicious node in the routes. The advantages of this approach are also compared with the traditional approaches that tend to use other criteria such as shortest path alone. Using OPNET simulator, the proposed approach is validated and further studied. The findings show that when the proposed approach is utilized, the overall performance of the Ad-hoc network is significantly improved.**

Keywords—Ad-hoc networks, Behaviour, Malicious attacks, Simulation, Throughput

I. Introduction

A wireless Ad-hoc network consists of a group of wireless devices that are capable of communicating with each other without the need for any central management infrastructure. Such a capability, along with the mobile nature of these networks, provides many advantages. However, these same characteristics are the root of several nontrivial challenges in securing such networks [1]. In these networks, nodes are free to move and organize themselves in a capricious fashion. To communicate, multi-hop routing capability is required for nodes that are not within radio range of each other. That is, each node may need to act as a router, forwarding packets to other nodes [2]. Ad-hoc networks can be used in a wide variety of environments and applications, where an infrastructure is not available. A key feature of these networks is their ease of deployment, which makes them suitable for military fields, disaster and rescue operations, conferences, as well as home and mesh networking.

A major challenge in Ad-hoc networks relates to their inherent lack of security. The open architecture of the network, coupled with the constantly changing topology, and the accessibility to the wireless channel by both genuine network users and malicious attackers, have limited the users trust to rely on these networks. Also, the lack of any centralized architecture or authority, can limit the use of many conventional security solutions, such as those based on traditional public key infrastructure, which are designed around a centralized mechanism [3].

In Ad-hoc networks, a node may be considered as misbehaving for different reasons, for instance when it refuses to forward packets. In some circumstances, the node can be overloaded, which affects the CPU cycles, buffer space, and available bandwidth to forward packets. Nodes have also been known to save available resources by not forwarding packets unless they are of direct interest to the node itself. Conversely, these nodes may still be expecting others to forward packets on their behalf [4].

In our previous works, performance evaluation and simulation validation of Ad-hoc networks using OPNET Modeler have been reported [5]. In this study, we expand those works to include the effects of the presence of malicious nodes in an Ad-hoc network. This includes the measurement of the throughput, round-trip delay, and packet loss rate. Simulation results relating to malicious nodes producing both UDP and TCP malicious traffic are collected and analyzed. Based on the results of those analyses, an approach that utilizes the behaviour history of the network nodes is proposed. The main aim of this approach is to identify a route from source node to destination node that is free of malicious nodes.

To achieve this, the remainder of this paper is organized as follows. Some of the security deficiencies in traditional Ad-hoc networks are given in Section 2. In Section 3, an overview of the proposed approach is presented. An outline of the simulation setup together with various scenarios used in this study are presented in Section 4. Collected results and their analysis are discussed in Section 5 which is followed by concluding remarks in Section 6.

II. Security Deficiencies in Ad-hoc Networks

Strictly speaking, although the term is usually used to refer to a node that attempts to disrupt, destroy or destabilize a network, a malicious node is any node that weakens or reduces a network's capability to perform its expected function [6].

Identifying the most popular malicious attacks in Ad-hoc networks is the first step towards the development of any trust evaluation system. One simple form of malicious node is one that drops packets. This node can still participate in lower-level protocols, but it drops packets on a random basis. This causes the quality of the connections to become aggravated and can further have a negative effect on the performance if TCP is the transport layer protocol used [7]. Forwarding messages along wrong paths is another form of malicious nodes. These nodes tend to divert packets away from their intended destination, which may lead to a DoS attack. Malicious nodes can also fabricate and transmit falsified routing messages to mislead other routes and to create invalid paths in their routing tables. These types of nodes advertise false routing messages to every other node, forming a black-hole and a wormhole within the network [8]. As their advertisement propagates, the network routes more traffic in their direction. The effects could lead to route failures and thus affect the overall performance of the Ad-hoc network. A malicious node can launch a replay attack by sending stale updates to some node, in an attempt to get that node to update its routing table using out of date routes. This can also lead to degradation in the performance of the Ad-hoc network. These types of malicious nodes have been referred to in several papers [6-11].

Significant work has been done to improve routing in wireless Ad-hoc networks. Some of them apply a reputation technique to face malicious nodes. Others make use of the public and symmetric key infrastructure by designing secure routing solutions. To date, improvements in relation to this issue is still an ongoing investigation [12] and [13]. Many important problems and challenges still need to be addressed. These include the absence of a fixed infrastructure and centralized administration, as key management becomes a complicated problem and in turn making it difficult to provide proper security solutions [14]. To mitigate this problem, an approach which is based on account and reputation mechanisms to motivate nodes in an Ad-hoc network has been studied [15]. The use of digital signature for authentication by each node has also been considered [16]. However, this solution assumes the existence of a trusted certificate server, which is not easily achievable, given the nature of Ad-hoc networks. A secure routing protocol which is based on symmetric key cryptography has also been proposed [9]. This approach is based on the assumption that the source node shares a secret key with the destination node. An extension to the Ad-hoc On demand Distance Vector (AODV) protocol to secure it was also proposed [17]. In this approach, it was claimed that the hop count information is the only mutual field in AODV and so used hash chains to secure this field. This approach also works under the presumption that an efficient key management system which distributes public keys to all nodes of the network is present. A watchdog that detects misbehaving nodes and a pathrater that evaluates paths based on the information collected by the watchdog was introduced [4]. Based on the characteristic that a node is able to overhear its neighbour communication, misbehaviour such as packet dropping is detected. Successfully detected malicious nodes are avoided by the pathrater. However, avoiding these nodes will not stop their previous outgoing data packets to be forwarded to the destinations. A new reputation scheme to identify malicious nodes was also proposed [18]. If a node fails to route the packet, it gets a low reputation and will be thrown out from the network. However the drawback of this approach is that for the good nodes to be credited, an acknowledgment which is sent by the destination has to be received first.

III. THE BEHAVIOUR HISTORY EMPLOYMENT

In our work, the main focus surrounds on-demand routing protocols, where the route is discovered only when a node wants to send data to another node. The routing protocol used in this study is the AODV protocol. When a node wants to send data to another node, it broadcasts a Route Request (RREQ) packet to all its neighbours. The RREQ propagates through the network until it reaches the destination or a node with a fresh enough route to the destination. Forwarding of RREQs is done when the node receiving a RREQ does not have a route to the destination. It then rebroadcasts the RREQ. This process is repeated until the RREQ reaches the destination which sends a Route Reply (RREP) back to the sender. When a node detects that a route to a neighbour is no longer valid, which may be caused by a link break, it removes the routing entry and sends a Route Error (RERR) message to the neighbours that are actively using the route, informing them that this route is no longer valid. This procedure is repeated until the message reaches the source where it either stops sending data or requests a new route by generating a new RREQ. A detailed description of this protocol can be found in [19].

In the proposed scheme, the source node tends to find a route to the destination that enclose less number of malicious nodes as opposed to the traditional protocols that aim to choose the shortest route. To achieve this, a new parameter is added to the routing protocol to record the behaviour of a node. This parameter is a function of the packets relayed by this node. These include control packets as well as data packets. In the initial stage, this parameter is the same for all nodes. Every time a node forwards a packet (either data or control packet) the parameter is incremented. Conversely, whenever a node fails to relay a packet, the parameter is decremented. Therefore, the more packets forwarded by a node the more reliable this node will be. This level of reliability allows this node to be chosen by other nodes. On the other hand, the fewer packets a node forwards, the less trusted this node will be and thus will not be used to forward packets to other nodes. When a node wants to communicate with another node, it finds a set of routes to the destination using one of the on-demand routing protocols. The source node then forwards the packet to the neighbour node with the highest value of the behaviour parameter. In the case where two neighbour nodes have the same behaviour value, the source will choose the node corresponding to the route with the less number of hops. The source node then checks if the corresponding node forwards the packet or drops it using the promiscuous capability of the wireless cards. In the first case the behaviour parameter of this node will be incremented otherwise it ends up being decremented. The different aspect of this scheme when comparing it to the scheme in [18] is that the node does not wait to receive an acknowledgment sent by the destination in order to update the behaviour parameter. Instead the update is done after the node forwards the packet. This specific

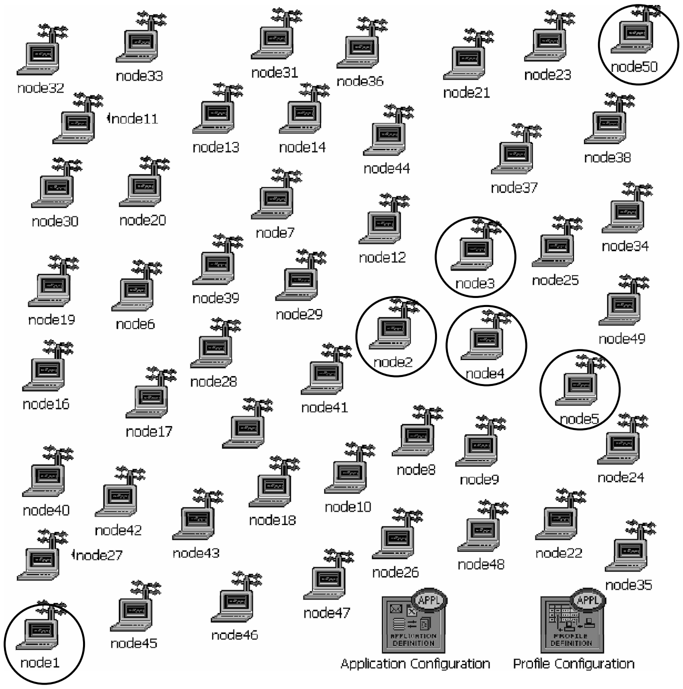

Figure 1. A snapshot of the OPNET simulation setup

technique solves the problem of not receiving the acknowledgment which may occur due to varying reasons. In this case the whole route will get a negative behaviour for a reason which is not caused by a malicious attack. Further if an intermediate node drops the packet, it will not affect all the nodes in the corresponding route. This process is repeated until the packet reaches the destination node. It should be noted here that the possibility of an intermediate node forwarding the packet to a third node that is not a part of the route to deceive the originator node is not considered.

IV. Simulation Study Setup

The simulation is carried out using OPNET Modeler V11.5 OPNET Modeler is used to construct models for two different purposes: to study system behaviour and performance; and to deliver a modeling environment to end users [20] A network model may contain any number of communicating entities called nodes. Nodes are instances of node models; developed using the Node Editor. Network models consist of nodes and links that can be deployed within a geographical context. Node models consist of modules and connections.

Each simulation scenario consists of fifty nodes. The channel speed of the wireless LAN is set to 11 Mbps. The routing protocol used in the simulation is the AODV protocol

To study the effects of the presence of malicious nodes in Ad-hoc networks, three performance metrics will be measured for a number of scenarios and situations. These are the throughput, the round-trip delay, and the packet loss rate. the total measured throughput is considered as the average amount of data payload transmitted and received over a period of time between two nodes. It is measured in Mbps. The packet loss percentage at nodeX for transmission between nodeX and nodeY describes the percentage of packets transmitted from nodeX over the network that did not reach nodeY. The round-trip delay refers to the average time taken by a packet to complete one full trip from source to destination and back and is measured in msec.

TABLE I Description of the scenarios used

	Description
Baseline Scenario	**only two nodes involved in the communication, node2 is sending TCP traffic to node4**
First Scenario	**node2 and node3 are communicating simultaneously with node4 sending TCP traffic**
Second Scenario	**node 4 is receiving TCP traffic generated and sent at the same time from node2, node3, and node5**
Third Scenario	**node2 is sending TCP traffic to node5 (node2 is not within the range of node5 so node2 uses other nodes as relay nodes)**
Fourth Scenario	**node1 is sending TCP traffic to node50 (all nodes are motionless)**
Fifth Scenario	**node1 is sending TCP traffic to node50 (all nodes are mobile at a speed of 10m/s following a defined trajectory)**

The simulation study consists of number of scenarios replicating practical situations. In the first part we concentrate on the effects of malicious nodes trying to interfere with the communicating nodes by sending background traffic. Each scenario is running in five different situations. In the first situation, no malicious nodes are present in the network's fifty nodes, and only nodes involved in the communication are sending and receiving data. In the second situation, five random nodes out of the fifty nodes are malicious nodes. Ten malicious nodes are present in the third situation, whilst in the fourth; fifteen nodes are considered malicious nodes. In the fifth situation, twenty out of the fifty nodes are malicious nodes. Figure 1shows a snapshot of the simulation setup.

In the baseline scenario, only node2 and node4 are involved in the communication. TCP traffic is sent from node2 to node4 and the throughout, packet loss rate and round-trip delay are measured at node2. In the first scenario node2 and node3 are set up to send TCP traffic to node4. While in the second scenario node5, node3, and node2 are communicating simultaneously with node4. In the third scenario node2 is sending traffic to node5 through other nodes acting as relay nodes between the source and the destination.

Several simulations have been performed in order to investigate the behaviour of transport layer protocols, both TCP and UDP when used by the malicious nodes. To achieve this, the simulations are run in two different situations. In the first situation, the malicious nodes are sending TCP traffic, whilst in the second situation the malicious nodes are sending UDP traffic.

In the second part of simulation we have tried to make the situation more random and general by changing the way malicious nodes are acting. Thus four categories of malicious

TABLE II Throughput comparison for the baseline, first, second and third scenarios measured in Mbps

	Malicious TCP Traffic (Measured in Mbps)	Malicious UDP Traffic (Measured in Mbps)
Baseline Scenario	4.59	4.79
First Scenario	2	2.14
Second Scenario	1.67	1.47
Third Scenario	1.71	1.83

nodes are defined here. In the first type, malicious nodes are dropping packets based on the simulation time (for example dropping all packets when the simulation time is between 50 and 100 sec). In the second group, malicious nodes are dropping every second packet, while in the third type nodes are dropping every fifth packet. For the last category, nodes are dropping every eighth packet. To also study the effect of nodes mobility on the performance of Ad-hoc networks, all nodes are moving randomly 60 sec after beginning of simulation with a speed of 10 m/s. Nodes move for 20 sec, pause at their destination for 60 sec and back to their original locations. Similarly, within each scenario there exist five stages corresponding to zero, five, ten, fifteen, and twenty malicious nodes respectively. Two scenarios were defined for this part. In the fourth scenario, node1 is sending TCP traffic to node50 through other nodes that are acting as relay nodes. All nodes in this scenario are wireless fixed nodes, while in the fifth scenario all nodes are moving according to the defined trajectory. TABLE I shows a brief description of the scenarios used.

V. Results and Analysis

All simulations run for five minutes. TABLE II shows the throughput variation values collected at node2 and when 40% of the nodes are acting maliciously. This table shows both situations where the malicious nodes are sending UDP and TCP traffic. It is clear from these values that the impact on the throughput is less when the malicious nodes are using UDP traffic rather than TCP traffic. This is attributed to the nature of TCP, which ensures that the data is delivered error free and in order. As the receiving node does not distinguish between malicious and data traffic, delays at node2 can be expected. This is in line with previously published results [4].

The graphs in Figure 2 show the round-trip delay variation for the baseline scenario. Again, the measurement is made at the sending node and the graphs show both situations where the malicious nodes are sending UDP and TCP traffic. It is noticeable from these graphs that the malicious nodes have affected the round-trip delay between the communicating nodes for this scenario. These graphs also indicate that the impact on the round-trip delay is less when the malicious nodes are using UDP traffic. This can be attributed to the use of the window mechanism to control the flow of data in TCP. When a TCP connection is established, each end of the connection allocates a buffer to hold incoming data. If the receiving application can read data as quickly as it arrives, the receiver will send a positive window advertisement with each acknowledgement. However, as expected if the sender is faster than the receiver, incoming data will eventually fill the receiver's buffer. Thus, as data and malicious traffic arrive at node2, node2 sends acknowledgements to each node causing delay and full buffer at node2. In this situation node2 advertises a zero window. A sender that receives a zero window advertisement must stop sending until it receives a positive window. The graphs for the first, second, and third scenarios show similar activity to those in Figure 2. For example the round-trip delay where twenty malicious nodes exist in the network has raised from 4.2 msec to 84.2 msec for UDP malicious traffic and 92.6 msec when the malicious nodes are using TCP as transport protocol for the second scenario.

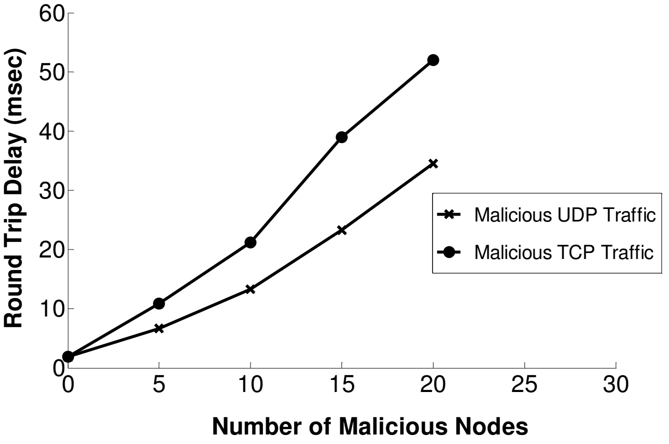

Figure 2. Round-trip Delay variation for baseline scenario measured at node2 for TCP and UDP malicious traffic

The graphs in Figure 3 show the packet loss percentage variation for the first scenario. Also the graphs show both situations where the malicious nodes are sending UDP and TCP traffic. It is also clear from these graphs that the packet

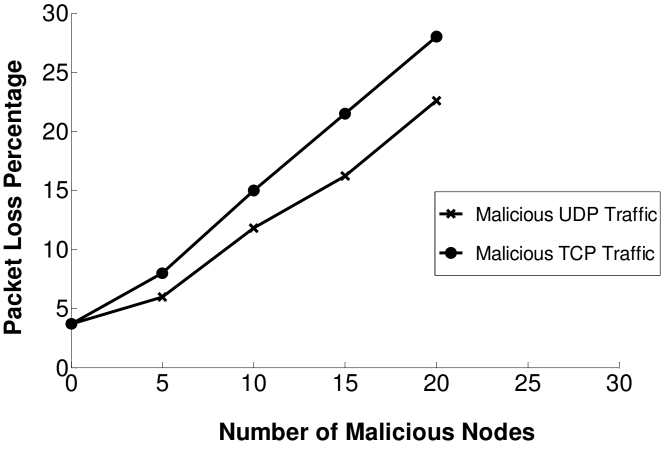

Figure 3. Packet loss percentage for the first scenario measured at node2 for TCP and UDP malicious traffic

TABLE III Packet Loss percentage comparison for the fourth and fifth scenario

	Without the Proposed Approach	With the Proposed Approach
Fourth Scenario (TCP data Traffic)	51%	45%
Fifth Scenario (TCP Data Traffic)	57%	49%

loss rate is affected by the presence of the malicious nodes in the network. Additionally, this is in line with previously published results [21]. These graphs also show that this performance metric is also plagued by the transport protocol that the malicious nodes are using. This might be attributed to the fact that malicious nodes are trying to retransmit their traffic when using TCP. This process at nodes2 cannot distinguish between normal and malicious traffic. So this can cause higher packet loss rate compared to when malicious nodes are using UDP. The performance of the baseline, second and third scenarios also show similar behavior to the first scenario. For example, the packet loss rate has raised from 0 to around 10% when twenty malicious nodes using UDP protocol are present in the network, compared to 15% when using TCP for the baseline scenario.

The following section displays the results of the second part of the simulation. As stated before, in this part node1 is sending TCP traffic to node50 via other nodes, which act as relay nodes. Several simulations were performed before and after applying the proposed approach in order to study the effect of the use of the behaviour history of the nodes on the overall performance.

TABLE III shows the packet loss percentage values measured at node50 before and after applying the proposed approach and when 40% of the nodes are acting maliciously. This table shows both situations when nodes are motionless (fourth scenario) and when nodes where moving according to the defined trajectory (fifth scenario). It is clear from these values that the packet loss has decreased with the proposed approach. This is due to the fact that node1 is now sending the packets to node50 through a route which has less malicious nodes. It is also noticeable that the packet loss is higher when the nodes are moving. This is due to the fact that when moving, the node can lose the connection with its neighbours causing the routing protocol to reinitiate the route between source and destination.

TABLE IV Throughput comparison for the fourth and fifth scenario measured in Kbps

	Without the Proposed Approach	With the Proposed Approach
Fourth Scenario (TCP data Traffic)	335	373
Fifth Scenario (TCP Data Traffic)	309	350

TABLE IV shows the throughput comparison for the fourth and fifth scenario when 40% of the nodes are acting maliciously. It is noticeable here that the throughput has increased with the proposed approach. The increase in the throughput can also be credited to the fact that the new route between source and destination has none, or less, malicious nodes. It can also be noted that the throughput is lower when the nodes are mobile.

OPNET Modeler provides several statistics during simulation execution to analyze the performance of the routing protocol used. The available AODV performance statistics are: Total Route Request Sent, Total Route Replies Sent, Total Route Errors Sent, Total Replies Sent from Destination, Total Packets Dropped, Total Cached Replies Sent, Routing Traffic Sent (Packet/Second), Routing Traffic Received (Packet/Second), Number of Hops Per Route, and Packet Queue Size. Routing Traffic sent defines the total number of routing traffic sent in packets in the entire network. This statistic was collected to check the amount of routing traffic generated by the network when using the proposed BAODV protocol as the routing protocol.

The graphs in Figure 4 show a comparison of the routing traffic sent in the entire network before and after applying the proposed approach for the fourth scenario. It is noticeable in these graphs that the amount of routing traffic sent in the entire network is higher when using the BAODV protocol. This is due to the fact that when a malicious node between a source and a destination node is detected, the routing path between these two nodes will change causing an increase in the routing traffic.

The graphs in Figure 5 show a comparison of the routing traffic sent in the entire network before and after applying the proposed behaviour for the fifth scenario. As expected, the amount of routing traffic is higher with the proposed approach. The same argument given for the fourth scenario can be given

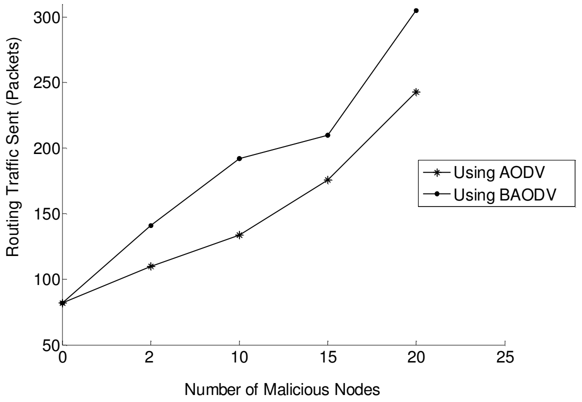

Figure 4 Routing Traffic Sent comparison for the fouth scenario. These graphs show both situations before and after applying the proposed approach

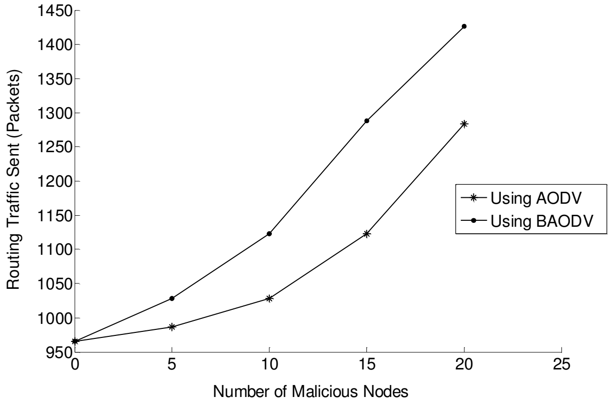

Figure 5 Routing Traffic Sent comparison for the fifth scenario. These graphs show both situations before and after applying the proposed approach

here. It is also noticeable when comparing the graphs in Figure 4 and Figure 5 that the amount of routing traffic is much higher when the nodes are moving. The most likely reason for this is that when moving, nodes can loose connections between each other causing the sending nodes to re-establish the corresponding routes with the destinations resulting in higher routing traffic.

VI. CONCLUSIONS

In this paper, an approach that utilizes the behaviour history of Ad-hoc network nodes to identify a secure and reliable route is proposed and examined. The route is established through exclusion of the nodes that may be considered to be malicious, based on their behaviour history. The results of throughput, round-trip delay, and packet loss rate, with some nodes acting maliciously have been studied. Data collections for different situations, where malicious nodes are sending TCP and/or UDP traffic are also carried out. Simulation studies, using OPNET, demonstrate that the malicious nodes sending UDP traffic have less negative impact on the overall performance of the network compared to when they send TCP traffic. The reported results clearly show that the overall performance of the Ad-hoc networks, even in the presence of malicious nodes, can be significantly improved by incorporating the behaviour history of the nodes. For instance, with 40% of the nodes of the Ad-hoc network acting maliciously, and nodes being either stationary or mobile, increases of 11% and 13% respectively in throughput values can be achieved. In future works, we plan to use these results in conjunction with soft computing approaches to further enhance security and reliability of Ad-hoc networks. It is well known that fuzzy logic offers the ability to handle uncertainty and imprecision effectively. Utilising fuzzy logic concepts, BAODV can be expanded to incorporate trust levels between the nodes of Ad-hoc networks.

ACKNOWLEDGMENT

We would like to thank OPNET for their kindness in providing us with Modeler software license, which has greatly assisted in finalizing this paper. We also would like to thank Cisco for the generous scholarship which has permitted us to move forward with our studies.

REFERENCES

[1] S. Dhar, "MANET: Applications, Issues, and Challenges for the Future," *International Journal of Business Data Communications and Networking*, 2005, vol. 1, pp. 66-92.

[2] K. S. Ng and W. K. G. Seah, "Routing security and data confidentiality for mobile Ad-hoc networks," I*n Proc. of the 57th IEEE Semiannual Vehicular Technology Conf. (VTC 2003-Spring),* 2003, pp. 1821-1825 vol.3.

[3] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile Ad-hoc networks: challenges and solutions," *Wireless Communications, IEEE*, 2004, vol. 11, pp. 38-47.

[4] A. S. Marti, A. T. J. Giuli, A. K. Lai, and A. M. Baker, "Mitigating routing misbehavior in mobile Ad-hoc networks," I*n Proc. of the 6th Int. Conf. on Mobile computing and networking, Boston, Massachusetts, United States,* 2000, pp. 255-265.

[5] H. Hallani and S. A. Shahrestani, "Performance Evaluation and Simulation Verification for Wireless Ad-hoc Networks," *WSEAS Transactions on Communications*, 2005, vol. 4, pp. 355-362.

[6] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, 2002, vol. 35 No.10, pp. 54-62.

[7] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks," *MILCOM*, 2002, pp. 1118-1123.

[8] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks," I*n Proc. of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02),* 2002, pp. 3-13.

[9] Y. Hu, A. Perrig, and D. Johnson., "Ariadne: A secure on-demand routing protocol for Ad-hoc networks," *Wireless Networks*, 2005, vol. 11, pp. 21-38.

[10] A. I. Aad, A. J.-P. Hubaux, and A. E. W. Knightly, " Denial of service resilience in ad hoc networks," I*n Proc. of the Proceedings of the 10th annual international conference on Mobile computing and networking, Philadelphia, PA, USA,* 2004, pp. 202-215.

[11] P. Rathod, N. Mody, D. Gada, R. Gogri, Z. Dedhia, S. Sanyal, and A. Abraham, "Security Scheme for Malicious Node Detection in Mobile Ad Hoc Networks," *Lecture Notes in Computer Science*, 2004, vol. 3326, pp. 541-542.

[12] G. C. Hadjichristofi, W. J. Adams, and N. J. Davis, IV, "A framework for key management in mobile Ad-hoc networks," I*n Proc. of the Int. Conf. on Information Technology: Coding and Computing, (ITCC 2005),* 2005, pp. 568-573 Vol. 2.

[13] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure Routing and Intrusion Detection in Ad-hoc Networks," I*n Proc. of the 3rd IEEE Int. Conf. on Pervasive Computing and Communications, (PerCom 2005),* 2005, pp. 191-199.

[14] C. E. Perkins, "Ad-hoc Networking," *Addison-Wesley*, 2000.

[15] P. Obreiter, B. Koenig-Ries, and M. Klein, "Stimulating Cooperative Behavior of Autonomous Devices - An Analysis of requirements and Existing Approaches", *2nd Int. Workshop on*

Wireless Information Systems (WIS2003), Angers, France April 2003.

[16] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated routing for ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, 2005, vol. 23, pp. 598-610.

[17] M. G. Zapata, *Secure ad hoc on-demand distance vector (saodv) routing* Internet Engineering Task Force (IETF) Draft, 2004.

[18] P. Dewan, P. Dasgupta, and A. Bhattacharya, "On using reputations in Ad-hoc networks to counter malicious nodes," I*n Proc. of the 10th Int. Conf. on Parallel and Distributed Systems, (ICPADS 04).* 2004, pp. 665-672.

[19] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," I*n Proc. of the Mobile Computing Systems and Applications,* 1999, pp. 90-100.

[20] OPNET Modeler, "http://www.opnet.com."

[21] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the CONFIDANT protocol," I*n Proc. of the 3rd ACM Int. Symposium on Mobile Ad-hoc networking & computing (MobiHoc 02), Lausanne, Switzerland,* 2002, pp. 226-236.