Fuzzy Trust Approach for Wireless Ad-hoc Networks

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— *A wireless Ad-hoc network is a group of wireless devices that communicate with each other without utilising any central management infrastructure. The operation of Ad-hoc networks depends on the cooperation among nodes to provide connectivity and communication routes. However, such an ideal situation may not always be achievable in practice. Some nodes may behave maliciously, resulting in degradation of the performance of the network or even disruption of its operation altogether. To mitigate the effect of such nodes and to achieve higher levels of security and reliability, this paper expands on relevant fuzzy logic concepts to propose an approach to establish quantifiable trust levels between the nodes of Ad-hoc networks. These trust levels are then used in the routing decision making process. Using OPNET simulator, the proposed approach is validated and further studied. The findings show that when the proposed approach is utilised, the overall performance of the Ad-hoc network is significantly improved.*

1. Introduction

Wireless networking has experienced fast development in the last few years. A large number of handhelds, portables, and mobile phones have become implanted with wireless communication capabilities [19]. As a result of this, very small computer devices with wireless communication capabilities will soon be embedded in almost every product. The mobility and the freedom offered by these wireless devices allow users to remain connected to their enterprise networks, while on the move [12].

Modern Wireless Local Area Networks (WLANs) with relatively high data rates have become an attractive technology for providing Internet connectivity for mobile users. Professional deployment of WLANs requires the capability to broaden the coverage without the need to deploy a costly infrastructure [4]. Ad-hoc based wireless networks are an attractive solution for this problem. A wireless Ad-hoc network can be considered as a group of wireless devices with radio frequency connectivity that assist each other in transmission of data packets within the network. Data traffic flows over one or more paths between succeeding nodes to reach its destination, making wireless Ad-hoc networks similar to the structure of the Internet [6]. A key advantage of Ad-hoc networks over conventional WLAN configurations is that Ad-hoc networks have no single point of failure [9].

Most modern networks are based on pre-established relationships between clients and service providers. In most cases, the movement of users from their established environment may cause various difficulties and problems. To overcome some of these difficulties, wireless Ad-hoc networks provide a number of solutions. The first of these relates to ease and simplicity. A node, which is capable of reaching one or more available neighbouring nodes, can be added easily to the network. Secondly, wireless Ad-hoc networks allow the users to overcome geographical and location limitations. This is due to the fact that all nodes in the network can provide connectivity as opposed to a single access point. Scalability is also an advantage as Ad-hoc networks are robust and can be easily scaled up. Finally, wireless Ad-hoc networks offer a significant cost saving, as the existing environment does not have to be modified drastically to accommodate the addition of nodes to the existing and evolving network. [2].

In our previous works, the effects of the presence of malicious nodes in an Ad-hoc network have been reported [8]. This included the introduction of the BAODV approach which utilises the behaviour history of the network nodes [7]. In this paper a new approach that is based on fuzzy logic concepts to optimise the evaluation of trust between nodes is introduced. Fuzzy logic provides a simple way to arrive at a definite conclusion based upon vague, ambiguous, or imprecise input information. Different factors and parameters should be identified and combined in order to determine if a node is acting maliciously. Incorporating trust in Ad-hoc routing protocols and thereby mimicking human behaviour can facilitate the detection of nodes that misuse the trust placed in them.

To achieve this, the remainder of this paper is organized as follows. The motivations for using fuzzy logic concepts to evaluate trust levels between nodes in an Ad-hoc network are presented in Section 2. In Section 3, a detailed description of the fuzzy trust algorithm is illustrated. 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.

2. Motivations

In the last few years, different routing protocols for Ad-hoc networks have been proposed. But most of them tend to ignore the fact that all the nodes in the network will not necessarily fully cooperate in routing the packets from source to destination. In general, many Ad-hoc devices operate on battery power. Consequently, power consumption for each transmission has a certain cost and significance. So, in reality, the assumption that all nodes perform the task of forwarding data, from which they do not directly benefit, while

consuming their own battery power, is not always achievable [20]. There is little reason to assume that some nodes will not try to achieve the benefits of participating in the network and avoid the disadvantages it involves. This could mean that some nodes may refuse to forward packets as expected and thereby decrease the efficiency of the network. Due to the dynamic nature of Ad-hoc networks, identifying nodes that express such malicious behaviour is a difficult task. The node originating the transmission might be out of range for detecting the malicious act [5].

The open structure, lack of existing infrastructure and inaccessibility to trusted servers make traditional security methods and systems insufficient for Ad-hoc networks. This problem, faced with the presence of malicious nodes in Ad-hoc networks, requires the existence of a trust level based algorithm to alleviate the effect of such nodes [3]. To address this problem an approach arising utilising fuzzy logic concepts to establish trust relationships between nodes is proposed. To facilitate the quantification of trust levels for a node, information about the behaviour history of this node is collected. Incorporating the concept of trust in Ad-hoc routing protocols and thereby mimicking human behaviour, can further improve the performance and the reliability of Ad-hoc networks. It is expected that the establishment and quantification of trust levels can be used to detect nodes that misuse the trust placed in them. The detection of misbehaving nodes can be used to apply trust based route selection strategies to Ad-hoc routing protocols and thereby increase the effectiveness of the network. Four types of misbehaving nodes are considered in this paper. These include nodes that drop packets randomly, forward packets to the wrong destination, fabricate and transmit falsified routing messages, and launch replay attacks.

The trust level that can be assigned to a node is obviously not a crisp value, due to the multiple factors that can affect the trustworthiness of the nodes. Therefore, combining information related to these attacks by monitoring the neighbouring nodes can facilitate the quantification of trust levels. Thus, a model utilising fuzzy logic concepts is developed. To assign trust levels to nodes of Ad-hoc networks, a fuzzy trust evaluation application is developed using MATLAB [13]. This application receives information about the behaviour history of Ad-hoc network nodes. The trust levels are then used by the routing protocol in an attempt to choose the most reliable route between the source and the destination nodes. This approach is implemented and tested to show its benefits and drawbacks.

3. Overview of the Fuzzy Trust Algorithm

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. A detailed description of this protocol can be found in [18].

In human relationships, trust is often expressed linguistically rather than numerically [16]. Trust plays an important role in the cooperation and interaction between real world entities. It is well established that fuzzy logic is suitable to quantify trust among entities that comprise a network or a group. One of the advantages of using fuzzy logic to quantify trust between nodes in Ad-hoc networks is its ability to quantify imprecise data or uncertainty in measuring the security index of Ad-hoc nodes. In Ad-hoc networks, the trust level is affected by the past behaviour of the nodes. A node that in the past demonstrated dependability and responsiveness will gain increasing trust [1]. On the other hand, the unwillingness of a node to cooperate with other nodes will affect its trust level. In the proposed fuzzy trust evaluation model, the trust level of a node is determined by the percentage of packet dropped, the percentage of packets forwarded to the wrong destination, the number of replay attacks generated by this node, and the number of false routing messages produced by this node. These percentages are treated as fuzzy input variables. The output variable is the trust_level.

In the proposed Fuzzy Trust Algorithm (FTA), each route has a trust level. The route trust level is determined on the basis of the node which has the lowest trust level in that route. The main goal of FTA is to choose the most reliable route between the source and the destination. This is achieved by choosing the route with the highest trust level between the source and the destination nodes. In other words, the route with the highest trust level is comparably the most secure route.

When a source node S desires to transmit a data packet to a destination node D, S must acquire the next hop node along the path to D. If this information is not readily available then route discovery is performed on demand. In a typical Ad-hoc situation, there are R1, . . . , Rn, totally n possible routes from the source S to the destination D. In each route there exist an x number of relay nodes n_1, . . . , n_j , . . . , n_x to help in forwarding the packets from S to D.

After applying the fuzzy trust evaluation model each node will have a trust level. Each node is assumed to be able to evaluate the trust level of each of its neighbouring nodes based on the information regarding the behaviour history of these nodes. These trust levels are then used to determine the most appropriate route between S and D. Suppose the current trust level of the j^{th} node in the i^{th} route which is evaluated using the fuzzy trust evaluation model is T_{ij}, then the trust level of the i^{th} route is defined as the minimum trust level of all the nodes that are included in the i^{th} route:

$$(\text{trust level})_i = \min T_{ij},\ j \in (1, \ldots, x).$$

FTA utilises the trust levels to choose the most reliable route between the source node S and the destination node D. According to the AODV routing protocol, the source node S can receive more than one reply in a period of time after sending a RREQ. Those routes from S to D will all include a trust level value. The route with the maximum value of the trust level is then selected. As a result, the desired route "k" can be obtained as the route with the maximum trust level:

$$(\text{trust level})_k = \max (\text{trust level})_i ,\ i \in \{R1, R2, \ldots, Rn.\}$$

The FTA is based on a source-initiated on-demand routing protocol, so nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges. This type of routing creates routes only when requested by the source node. When a node requires a route to a destination, it initiates a route discovery process within the

network. This process is completed once a route is found or all possible routes trust levels have been examined. Once a route has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or until the route is no longer desired [14]. The FTA uses the following fields with each routing table entry: Destination IP Address, Destination sequence number, valid destination sequence number flag, trust level, hop count, next hop, and lifetime (expiration or deletion time of the route).

When S wants to send a message to D, and does not already have a valid route to that destination, it initiates a path discovery process to locate other nodes. The source node S propagates a RREQ to its neighbours. The RREQ packet includes: The IP address of D, the sequence number of D, trust level (the minimum trust level of all nodes in the current found route), hop count, and lifetime. The destination sequence number field in the RREQ message is the last known destination sequence number for this destination and is copied from the destination sequence number field in the routing table. If no sequence number is known, the unknown sequence number flag must be set. The trust level field is equal to the source node's trust level. The hop count field is set to zero. When a neighbour node receives the RREQ packet, it will be forwarded if it matches some conditions.

When an intermediate node receives the RREQ from its neighbour, it first increases the hop count value in the RREQ by one. This is to account for the new hop through the intermediate node if the packet is not going to be discarded. The originator sequence number contained in the RREQ must be compared to the corresponding destination sequence number in the routing table. If the originator sequence number of the RREQ is greater than the existing value, the intermediate node compares the trust level contained in the RREQ to its current trust level to get the minimum. The intermediate node then updates the trust level of RREQ with the minimum. At this stage, the updated trust level of the RREQ is the trust level of the route. If the originator sequence number contained in the RREQ is greater than the existing value in its routing table, the relay node creates a new entry with the sequence number of the RREQ. If the originator sequence number contained in the RREQ is equal to the existing value in its routing table, the trust level of the RREQ must be compared to the corresponding trust level in the routing table. In the case that the trust level contained in the RREQ is greater than the trust level in the routing table, the relay node updates the entry with the information contained in the RREQ. During the process of forwarding the RREQ, intermediate nodes record the addresses of neighbours from which the first copy of the broadcast packet was received in their routing tables. This in turn establishes a reserve path. If additional copies of the same RREQ are received later, these packets will be discarded

Once the RREQ reaches the destination D or an intermediate node with a valid route to D, the destination or intermediate node generates a Route Reply (RREP) packet and unicasts it back to the neighbour from which it received the RREQ. In the case where the generating node is the destination itself, it must update its own sequence number to the maximum of its current sequence number and the destination sequence number in the RREQ packet originating the RREP. The destination node places its sequence number into the destination sequence number field of the RREP and enters the value zero in the hop count field of the RREP. When generating a RREP message, a node copies the destination IP address, the originator sequence number and the trust level from the RREQ message into the RREP message.

When an intermediate node receives the RREP from its neighbour, it first increases the hop count value in the RREP by one. As the RREP is forwarded back along the reverse path, the hop count field is increased by one at each hop. Thus, when the RREP reaches the source, the hop count represents the distance, in hops, of the destination node D from the source node S. The originator sequence number contained in the RREP must be compared to the corresponding destination sequence number in the routing table entry. If the originator sequence number of the RREP is greater than the existing value, the node compares the trust level contained in RREP to its current trust level to get the minimum, and then updates the trust level of RREP with that minimum. This minimum value represents the trust level of the route.

4. Simulation Study Setup

The simulation is carried out using OPNET Modeler V11.5 [11] 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 [17] 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. Fig. 1 shows a snapshot of the simulation setup.

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. In order to facilitate the comparisons between the different approaches, all performance parameters are combined into one indicative index. The Overall Performance Index (OPI) is calculated as the weighted sum of the three performance metrics that have been considered so far. The sum of the weights $w_t + w_{pl} + w_d$ is equal to 100%. The OPI is defined using the following formula:

$$OPI = w_t * Throughput\_Ratio + w_{pl} * Packet\_Loss\_Ratio + w_d * Round\_Trip\_Delay\_Ratio$$

where w_t, w_{pl}, and w_d are the weights corresponding to the throughput, the packet loss rate and the round trip delay metrics respectively. Throughput_Ratio, Packet_Loss_Ratio, and Round_Trip_Delay_Ratio are the ratio of the measured values to the nominal values. Distributing the weights between the three performance metrics can differ from one application to another. For example, packet loss has a higher impact on audio and video based applications than the throughput and the round trip delay. However, it is well known that the packet loss usually has more effect on the performance of Ad-hoc networks. Packet loss results in packet retransmissions which reduces throughput and increases round trip delay between nodes. Therefore, the

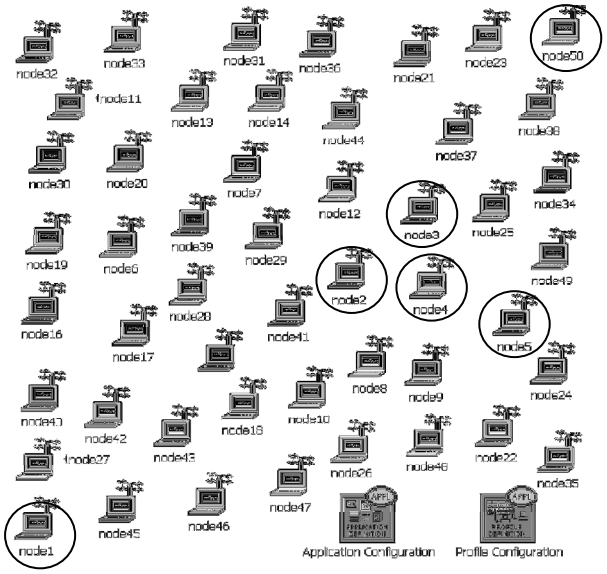

Fig.1. A snapshot of the OPNET simulation setup

weight for the packet loss parameter has been chosen to be twice that of the throughput and the round trip delay. As a result of that the weights are distributed as follows: $w_t = 25$, $w_d = 25$, $w_{pl} = 50$.

The simulation studies consist of a number of scenarios replicating practical situations. Each scenario runs in five different situations. In the first situation, none of the fifty nodes of the Ad-hoc network acts maliciously. In the second situation, five nodes chosen randomly out of the fifty nodes are acting maliciously. In the third situation, ten malicious nodes are present. In the fourth situation, fifteen nodes act as malicious nodes. In the fifth situation, twenty out of the fifty nodes are malicious nodes. The malicious nodes are implemented in four different ways. Some malicious nodes drop packets based on the simulation time (for example dropping all packets when the simulation time is between 50 and 100 sec). Other malicious nodes forward some of the packets to the wrong destinations. Some other malicious nodes fabricate and broadcast false routing messages. Other malicious nodes launch replay attacks. Also, to study the effect of nodes mobility on the performance of Ad-hoc networks, all nodes move randomly 60 sec after the start of each simulation with a speed of 10 m/s. The rationale behind waiting for 60 seconds before the nodes start to move is to give them a reasonable time to establish their routing tables. Nodes move for 20 sec, pause at their destination for 60 sec and move back to their original locations.

Scenarios

Four scenarios are applied in the evaluation of the FTA approach. In these scenarios node1 sends traffic to node50 using other nodes as relay nodes. In the first scenario, node1 sends TCP traffic to node50 through other nodes that are acting as relay nodes. In the second scenario node50 receives TCP traffic generated and sent from node50 through other nodes that are acting as relay nodes. All nodes are moving according to the trajectory described in the previous section. To check the effect of the transport layer protocol used between the communicating benign nodes on the performance of the Ad-hoc network, the same scenarios are repeated when the communicating benign nodes send UDP data traffic. Therefore, In the third scenario node50 receives UDP traffic sent from node1, using some nodes which are acting as routers forwarding packets to the destination node. In the fourth scenario node1 sends traffic to node50. All nodes are moving according to the trajectory defined in the previous section.

5. Collected Results and Analysis

A detailed analysis of an Ad-hoc network simulation results after applying the FTA approach are presented in this section. The variations of the throughput, round trip delay and packet loss are analysed individually. In most cases, the performance results of the evaluations metrics are plotted as graphs for easy comparison and quick reference. All simulations run for five minutes and the results are the average of repeating each simulation ten times.

Throughput Measurements

The results of the throughput measurements after applying the new FTA approach are reported here. In Fig. 2, the number of malicious nodes is plotted against the throughput for the first scenario. These graphs show both situations before and after applying the proposed FTA approach. These simulations are carried out with the number of malicious nodes varying from nil to 40% of the total number of nodes. Graphs for the other scenarios show similar behaviour. These graphs show that the proposed FTA approach can achieve up to 30% improvement in the throughput over the AODV protocol. This can be described by noting that the number of malicious nodes existing in the route between the communicating benign nodes is less in the FTA approach compared to AODV. This is due to the fact that, with more malicious nodes existing in the route, data from source to destination are more vulnerable to attacks, causing the deterioration of network performance. From these graphs, it is also evident that the improvements in the throughput values that can be achieved after applying the FTA approach are more pronounced when the network contains a larger number of malicious nodes. This can be explained by the fact that, as the number of malicious nodes increases, the number of reliable routes decreases. With five or more malicious nodes, however, reliable routes become rare, making it extremely likely to encounter a malicious node on the path. For instance, when a route consists of six nodes and 40% of the nodes are acting maliciously, then the probability that any route does not contain more than one malicious node is: $(0.6)^4 = 0.1296$ which means that only one out of eight routes is reliable.

Round Trip Delay Measurements

This section analyses the round trip delay measurement between communicating benign nodes after applying the FTA approach. In this thesis, the round trip delay measurement is considered as the average time taken to complete one full trip from source to destination and back. The graphs in Fig. 3 show the round trip delay variations for the first scenario. These graphs also show the situations before and after applying the FTA approach. This simulation is done with the number of malicious nodes changing from 0 to 20 nodes. It is clear from these graphs that when applying the FTA approach the average time for a given packet to complete a full round

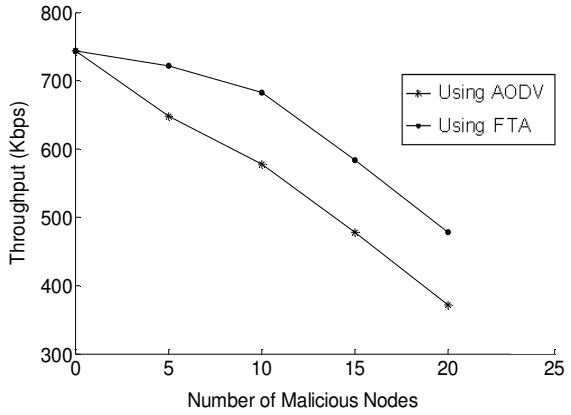

Fig. 2 Throughput comparison for the first scenario between AODV and the proposed FTA

trip between node1 and node50 is relatively lower. This applies to all scenarios. As mentioned in the previous section, the main reason for this behaviour is that the new route between source and destination has either no, or less malicious, nodes. When using the AODV protocol, as the number of malicious nodes increases, the total expected area covered by their radios increases and the likelihood of even a single reliable route existing decreases. On the other hand, by using the trust levels of the Ad-hoc network nodes, the FTA approach is able to find more reliable routes. From these graphs it can also be noted that, as the number of malicious nodes gets higher, the improvements in the round trip delay after applying the FTA approach are more achievable. This is mainly due to the fact that the higher the percentage of malicious nodes, the higher the probability that these nodes will participate in the route between the benign nodes. This can lead to more route request messages being dropped, causing a delay at the sending node [10].

Packet Loss Rate Measurement

The analysis presented in this section discusses the results of the packet loss rate after applying the FTA approach. The results in **Error! Reference source not found.** show the packet loss rate values for the first, second, third, and fourth scenarios when 40% of the nodes are acting maliciously. As in the previous measurements, the results cover situations

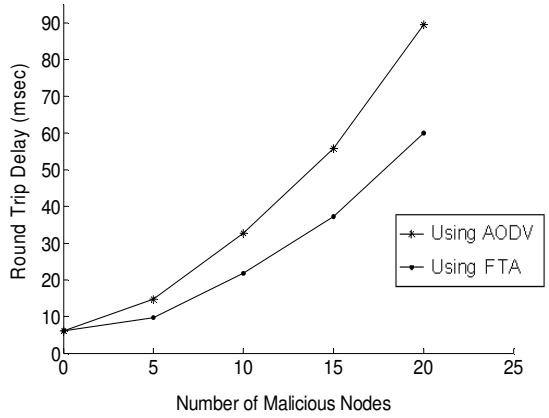

Fig.3 Round trip delay for the first scenario between AODV and the proposed FTA approach

Table 1: Packet loss comparison after applying the FTA approach

	Using AODV	Using FTA
First Scenario	51%	39%
Second Scenario	57%	45%
Third Scenario	44%	31%
Fourth Scenario	52%	38%

both before and after applying the proposed fuzzy trust based approach. It is noticeable here that there is a relatively higher packet loss rate experienced with the AODV protocol for all scenarios. For instance, the packet loss rate has decreased to 38% after applying the FTA approach, compared to 52% when nodes use AODV. The argument and explanation provided in the previous sections hold here. The decrease in the packet loss when using the FTA approach can be credited to the fact that the new route between the source and the destination has no, or less, malicious nodes. As a malicious node starts to launch attacks, its trust level becomes lower. Therefore, it is less likely to participate in the route between the communicating nodes and disrupt the operation of the network. It can also be noted that the packet loss rate is lower when the nodes are motionless. This can be attributed to the fact that packets are dropped when connections are lost between moving nodes. As the mobility of nodes increases, the topology changes in the network become more frequent. This causes a decrease in the accuracy of the routing information maintained by the routing protocol [15]. Therefore, the packet loss rate shows a slow increase as the mobility of the nodes increases. In summary, it can be concluded that the decrease in performance is mainly due to communication failures which arise more frequently when nodes are moving. These results also clearly show that as the number of malicious nodes in the network increases, the improvements in the packet loss rate that can be achieved after applying the FTA approach are more significant. This is mainly due to the fact that the higher the percentage of malicious nodes, the higher the probability that these nodes will drop the routing data messages, leading to a higher loss rate. With a high number of malicious nodes and without using the fuzzy trust evaluation approach, the percentage of successfully established routes decreases.

Overall Performance Index Comparison

Table 2: OPI comparison after applying the FTA approach

	Using AODV	Using FTA
First Scenario	45.54	59.66
Second Scenario	52.5	67.59
Third Scenario	46.62	64.32
Fourth Scenario	54.08	72.99

The main goal of using the OPI is to facilitate the comparison between AODV and the proposed FTA approach. As stated in Section 4, the Overall Performance Index is defined as a weighted sum of the throughput, round trip delay and packet loss parameters. Table 2 shows a comparison of the performance index before and after applying the FTA approach. These values clearly show the improvement in the Overall Performance Index that is achieved after applying the FTA approach. For instance, for the eleventh scenario and when 20 malicious nodes are present in the network, the OPI indicates a nearly 19% improvement.

6. Conclusions and Future Work

This paper has highlighted the importance of using trust levels to improve the reliability and performance of Ad-hoc networks. Evaluating trust levels between nodes of Ad-hoc networks poses a big challenge due to the lack of infrastructure in Ad-hoc networks. To overcome this limitation, a new approach based on fuzzy logic concepts is proposed to facilitate the evaluation of trust levels between nodes of Ad-hoc networks. Simulation and experimental results collected after applying the FTA approach show significant improvements in the performance and the reliability of Ad-hoc networks in the presence of malicious nodes. For instance, the OPI for the fourth scenario improved by 18.91% after applying the fuzzy trust based approach. However, a number of further investigations could be conducted to extend this approach. As stated in Section 2, human beings make many trust-based decisions on a subconscious level. Incorporating concepts similar to the way humans think into the FTA approach has the potential to further facilitate the evaluation of trust levels. Artificial Neural Networks for instance are used to perform tasks similar to those performed by human brains. The learning capability of Artificial Neural Networks made them a prime target for combination with fuzzy based systems in order to automate or support the developing process of such systems. Therefore, a future research direction would be to take advantage of the learning capability of Artificial Neural Networks by combining ideas and concepts evolving from such networks with the fuzzy trust based approach.

7. References

[1] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, "Reputation and Trust-Based Systems for Ad-hoc and Sensor Networks," *Algorithms and Protocols for Wireless Ad-hoc and Sensor Networks, A. Boukerche (ed.), Wiley & Sons*, 2007.

[2] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer Networks*, 2005, vol. 47, pp. 445-487.

[3] V. Balakrishnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, "Trust and Recommendations in Mobile Ad-hoc Networks," In *Proc. of the 3rd Int. Conf. on Networking and Services (ICNS 07), Athens, Greece,* 2007, pp. 64-69.

[4] E. Barka, "On The Impact of Security on the Performance of WLANs," *Journal of Communications*, 2007, vol. 2

[5] L. Fanzhi, S. Xiyu, J. Sabah, and A. Christopher, "The effects of malicious nodes on performance of mobile Ad-hoc networks," In *Proc. of the Mobile Multimedia Processing for Military and Security Applications,* 2006, pp. 1-6.

[6] T. Fowler, "Mesh Networks for Broadband Access," *IEE Review*, 2001, vol. 47, pp. 17-22.

[7] H. Hallani and S. A. Shahrestani, "Utilizing Behaviour History to fight malicious nodes in Wireless Ad-hoc Networks," In *Proc. of the 8th International Business Information Management Association (IBIMA) Conference, Dublin, Ireland,* June, 2007, pp. 84-89.

[8] H. Hallani and S. A. Shahrestani, " Wireless Ad-hoc Networks: Employing Behaviour History to Combat Malicious Nodes," In *Proc. of the 1st International Conference on Signal Processing and Telecommunication Systems (ICSPCS'07), Gold Coast, Australia,* December, 2007, pp. 1-6.

[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] S. A. Jafar, "Too Much Mobility Limits the Capacity of Wireless Ad-hoc Networks," *IEEE Transactions on Information Theory* 2005, vol. 51, pp. 3954-3964.

[11] X. Liu, "Application of OPNET in the Network Project and Design," *CONTROL AND AUTOMATION*, 2006, pp. 104-106.

[12] C. Mallett, W. Millar, and H. Beane, "Perspectives on Next Generation Mobile," *BT Technology Journal*, 2006, vol. 24, pp. 151-160.

[13] Matlab, "http://www.mathworks.com/products/matlab/."

[14] N. Meghanathan, "A Simulation Study on the Stability-oriented Routing Protocols for Mobile Ad-hoc Networks," In *Proc. of the Int. Conf. on Wireless and Optical Communications Networks,* 2006, pp. 1-5.

[15] N. Moghim, F. Hendessi, N. Movehhedinia, and T. A. Gulliver, "Ad-hoc Wireless Network Routing Protocols and Improved AODV," *Arabian Journal for Science and Engineering*, 2003, vol. 28, pp. 99-114.

[16] S. Nefti, F. Meziane, and K. Kasiran, "A Fuzzy Trust Model for E-Commerce," In *Proc. of the 7th IEEE Int. Conf. on E-Commerce Technology (CEC 05)* 2005, pp. 401-404.

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

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

[19] J. P. Shim, U. Varshney, S. Dekleva, and G. Knoerzer, "Mobile and Wireless Networks: Services, Evolution &

Issues," *IEEE International Journal of Mobile Communications Magazine*, 2006, vol. 4, pp. 405-417.

[20] X. Yang and N. Vaidya, "Priority Scheduling in Wireless Ad-hoc Networks," *Wireless Networks*, 2006, vol. 12, pp. 273-286.

Copyright © 2008 by the International Business Information Management Association. All rights reserved. No part or all of this work should be copied or reproduced in digital, hard, or any other format for commercial use without written permission. To purchase reprints of this article please e-mail: admin@ibima.org