Innovative Techniques for Attack Detection in Wireless Ad-Hoc Networks

Lamia F. Tulaib[1], Akbal O. Salman[2], Mazin A. Mohammed[3,*]

[1]College of Dentistry, University of Anbar, 31001, Anbar, Iraq

[2]Department of Control & Automation Techniques Engineering, Electrical Engineering Technical College, Middle Technical University, 06800, Baghdad, Iraq

[3]Information Systems Department, College of Computer Science and Information Technology, University of Anbar, 31001, Anbar, Iraq

Emails: den.lamia.faris@uoanbar.edu.iq; mazinalshujeary@uoanbar.edu.iq; akbal.o.salman@mtu.edu.iq

Abstract

As a result of the inherent weaknesses of the wireless medium, ad hoc networks are susceptible to a broad variety of threats and assaults. As a direct consequence of this, intrusion detection, as well as security, privacy, and authentication in ad-hoc networks, have developed into a primary focus of the current study. This body of research aims to identify the dangers posed by a variety of assaults that are often seen in wireless ad-hoc networks and provide strategies to counteract those dangers. The Black hole assault, Wormhole attack, Selective Forwarding attack, Sybil attack, and Denial-of-Service attack are the specific topics covered in this proposed work. In this paper, we describe a trust-based safe routing protocol with the goal of mitigating the interference of black hole nodes while routing in mobile ad-hoc networks. The overall performance of the network is negatively impacted when there are black hole nodes in the route that routing takes. As a result, we have developed a routing protocol that reduces the likelihood that packets would be lost because of black hole nodes. This routing system has been subjected to experimental testing to guarantee that the most secure path will be selected for the delivery of packets between a source and a destination. The invasion of wormholes into wireless networks results in the segmentation of the network as well as a disorder in the routing. As a result, we provide an effective approach for locating wormholes by using ordinal multi-dimensional scaling and round-trip duration in wireless ad hoc networks with either sparse or dense topologies. Wormholes that are linked by both short-route and long-path wormhole linkages may be found using the approach that was given. To guarantee that this ad hoc network does not include any wormholes that go unnoticed, this method is subjected to experimental testing. To fight against selective forwarding attacks in wireless ad-hoc networks, we have developed three different techniques. The first method is an incentive-based algorithm that makes use of a reward-punishment system to drive cooperation among three nodes for forwarding messages in crowded ad-hoc networks. A unique adversarial model has been developed by our team, and inside it, three distinct types of nodes and the activities they participate in are specified. We have demonstrated that the proposed method that is based on incentives prevents nodes from adopting individualistic behaviour, which ensures cooperation in the process of packet forwarding. In the second algorithm, a game theoretic model is proposed that uses non-cooperative game theory to ensure that intermediate nodes in resource-constrained ad-hoc networks faithfully forward packets.

Keywords: Incentive-based algorithm; intermediate nodes; Adhoc networks; forward packets

DOI: https://doi.org/10.54216/IJWAC.030105
Received: March 23, 2021 Accepted: August 15, 2021

1. Introduction

1.1 Ad-hoc Network Utilizing Wireless Technology

Over the course of the last several decades, wireless networks and systems have been experiencing a transformation that can only be described as revolutionary. The idea of ubiquitous computing has emerged as one of the most active areas of investigation within the context of society for wireless computing. Individual users have access to all of the necessary information in this domain whenever and whenever it is requested by them [1]. A ubiquitous device cannot obtain wired communication with other ubiquitous devices at every place or at every time since it is not feasible. It's possible that centralized infrastructure won't always be accessible in some circumstances. Because of this, wireless ad-hoc networks have become necessary for the interconnection of gadgets that are so pervasive in today's society. There are many different kinds of wireless ad hoc networks, but two of the most essential ones are sensor networks and mobile ad hoc networks. The use of ad hoc networks is highly recommended in circumstances in which the establishment of infrastructure is either not feasible or not reliable. These kinds of networks are used in a broad variety of commercial, military, and other mission-critical settings and applications. When implemented in hostile environments, ad hoc networks are susceptible to the security risks that come with such environments [2, 3].

In the absence of a predetermined infrastructure, a collection of communication devices or nodes that are individually outfitted with transceivers and can connect with each other via the use of radio waves is known as an ad-hoc network. Each node in a wireless ad-hoc network will automatically locate its neighbors by using their communication range [4]. Because of their restricted communication range, ad-hoc networks are predicated on the fundamental premise that their nodes are unable to engage in direct dialogue with one another. As a result, there must be some intermediary nodes between 1 and 2. The following is a list of the main qualities that are associated with ad-hoc networks. Multiple wireless devices may instantly establish a network connection [5] with one another.

Because of the mobility of nodes, there are frequent shifts in the network's connectedness. It is possible to reconfigure nodes such that they function as routers. The initial expenses of setting up the network are cut down because of the network's decentralized control. Scalability [6] requires the installation of more nodes in order to function properly.

The use of ad hoc networks is highly recommended in circumstances in which infrastructure is either unavailable or not reliable. It is possible to install ad hoc network nodes in a random pattern or in a uniform pattern. Ad-hoc networks are useful in a wide variety of contexts, [7] including industrial settings, personal area networks, and military operations, amongst others.

1.1.1 Network of Sensors that Are Wireless

The Wireless Sensor Network (WSN) is made up of sensor-equipped nodes, which are referred to as sensors. These sensors keep an eye on their surroundings and send the data they collect back to the base station or to one or more trustworthy gateways, which are referred to as sinks. Nodes in a WSN may be reprogrammed in response to changing requirements, and the networks can support either a large or a small number of nodes per unit area. Sensors are put in a hazardous environment for military surveillance, environmental monitoring, etc. WSNs are rapidly becoming widespread systems and have a broad variety of applications, ranging from the automation of homes to the monitoring of borders [8]. It is often necessary for sensors to be able to self-organize in a dispersed fashion.

Due to their limited processing capability, memory, and energy supply, sensors are susceptible to malfunctions and malicious assaults such as message injection [9], eavesdropping, impersonation, and others. This is compounded by the harsh operating circumstances that they must endure. In their most fundamental form, wireless sensor networks are just ad hoc networks with more severe limitations. Techniques that are standard include tamper-proof hardware, [10] secure routing, public-key cryptography, and many more.

These low-end gadgets need the adoption of certain preventative measures for their lack of security. Attackers in WSN can target any layer, from the physical layer all the way up to the application layer.

DOI: https://doi.org/10.54216/IJWAC.030105
Received: March 23, 2021 Accepted: August 15, 2021

1.1.2 Mobile Asynchronous Beacon Network

A MANET is made up of independent mobile nodes that are able to connect with one another via the use of wireless networks. In addition, it's functioning of it does not need the establishment of any established infrastructure.

Mobile nodes have less memory and power than fixed nodes and have the ability to quit or join the network at will, which results in a topology change that is both quick and unexpected [11]. A totally symmetric environment is formed as a result of the fact that each node in a MANET has the same capabilities and characteristics, and hence shares the same responsibilities. As a result of fluctuations in bandwidth, wireless networks are much less dependable and stable than their cable counterparts. MANET setup does not need human interaction. In addition, the MANET environment is subject to a number of restrictions and inefficiencies, including fading, path loss, and interference.

There is a high rate of packet loss as a result of collisions, and there is frequent route breakdown as a result of mobility and interference. The unpredictable migration of nodes may often cause MANET to experience network splitting.

2. Related Work

In the following example, [12], a source node uses hop counts and trust values to set up a forwarding route as well as a backup route. The encounter time and successful cooperation frequency of a node are used in the computation of direct confidence in that node. In order to calculate the suggested trust of a particular node, the D-S theory is used. The routing decision is made based on the course of travel that has the highest trust value. This technique enhances both the pace at which packets are sent and the latency from beginning to finish. In spite of this, there is no investigation of the routing overhead carried by the network when rogue nodes are present.

[13] In which each node connects with its neighbours in order to get direct trust or combine the recommended trust presented a trust model.

The direct trust and the suggested trust of a node are both taken into consideration when calculating the node's overall trust level. The trust level of a node is included in the route request packet that it is attached to. The routing decisions are made based on the intermediary nodes that have the highest trust values. The algorithm, on the other hand, is not able to protect against a bad-mouthing assault or malicious nodes that are working together.

A dynamic trust system that makes use of trust updates and collaborative filtering [14]. The trust updating algorithm monitors the fluctuation of trust values and also takes into account the effects of time, age, and the elements of punishment and reward. By using collaborative filtering, this approach eradicates instances of phony-suggested trust. On the other hand, this technique is unable to identify dishonest suggestions.

The AODV protocol includes a mechanism for the detection of malicious nodes known as special guard nodes [15]. For the purpose of route selection, the trustworthiness of each node is determined, and a predetermined threshold is used in order to identify malicious nodes. On the other hand, this approach is susceptible to poor-mouthing assault as well as energy limits.

The behavior of a node is watched for a predetermined amount of time [16], and the trust is estimated by making use of a summary of the observed behavior. When it comes to the successful transfer of packets, each node in the network keeps an eye on the activity of its neighbors. A Single Intrusion Detection (SID) packet will be broadcast by a node in the event that any malicious activity takes place inside the network. This will ensure that all participating neighbors are aware of the malicious behavior. The approach needs a significant amount of memory in order to store the reputation of the nodes.

A Node-based Trust Management (NTM) method is presented in [17], and it takes into consideration a mobile agent system that is hosted on each individual node. Node Initiators (NIs), Trust Monitors (TMs), and Trust Evaluators are the three parts that makeup NTM (TEs).

[18] developed a protocol called Trust embedded AODV (T-AODV), which creates a safe route from beginning to finish by relying on the cooperation of nodes. The header of the RREQ packet has been expanded to include an additional trust level field. When an RREQ packet is received by an intermediate node, this trust field is updated as part of the process. The amount of trust that a specific node's neighbors

DOI: https://doi.org/10.54216/IJWAC.030105
Received: March 23, 2021 Accepted: August 15, 2021

have with regard to that node is used to choose which route to take. The T-AODV protocol is unable to identify hostile nodes that are conspiring together.

The TAODV routing protocol is an extension of the AODV routing protocol that safeguards the behaviors of routing in MANETs [19]. Opinions are used to determine levels of trust between nodes in TAODV. During cryptographic procedures, every node has the flexibility to specify its own opinion threshold on its own. The viewpoints are always evolving and are presented in a timely manner. This system has a lower computational cost than other schemes; nevertheless, it has a slower reaction time than other schemes when it comes to identifying rogue nodes.

In their paper [20], Sarkar and Datta suggested a route selection strategy for MANET that made use of the mobility factor. A trusted module is implemented in this system. It computes and compares the mobility of the nodes that are of concern, and then it produces a trust value. The evaluation of the trust is done in three stages: the startup stage, the update stage, and the re-establishment stage. When determining a node's level of trust, this technique does not take into account whether or not it has a history of losing packets. Along with a soft encryption system, the trust-based reputation system and multi-path routing that is presented in [21] are intended to create a secure routing method. This routing technique does not do any analysis of the safety elements of the soft encryption mechanism.

3. Proposed Methodology

The transportation and logistics industry has a significant impact on the financial situation of both developed and developing nations. It also has significant negative effects on the environment. As a result, a rising number of studies and investigations to optimize these activities have been carried out during the last several decades, particularly with regard to activities involving considerable traffic in metropolitan areas.

In point of fact, investments in deploying infrastructure are limited by space and financial constraints, while on the other hand, the number of cars is continually expanding. As a consequence of this, the most efficient methods are necessary in order to control and cut down on urban traffic. As a result of this focus, intelligent transportation systems (ITS) are emerging to improve the efficacy, safety, and use of transportation activities and infrastructure by utilizing the power of information and communication technologies as well as Micro-Electro-Mechanical-Systems.

Indeed, researchers and automobile manufacturers are most interested in developing smart transportation experiences such as urban smart parking management and the search and identification of charging stations for electric cars. Consumers are often referred to as either the drivers or the passengers in activities and applications that include transportation. The customers are requesting a variety of services, including the sharing of information about accidents that have occurred, the monitoring and tracking of road health, weather report services, the measurement of traffic flow, the calculation of travel time, the sharing of audio and video, an intelligent interactive panel for driver assistance, and other similar services.

It is very necessary to establish a comprehensive VANET routing issue in order to give a higher Quality of Service (QoS) to the customers of ITS. This problem description for routing should identify and take into account the common ideas and restrictions of all real-world VANET applications, difficulties, concerns, and needs. When designing an efficient routing scheme for VANET, the most important factors that need to be taken into consideration are cooperation and collaboration between vehicles, as well as simultaneous consideration of time and space. These factors must be taken into account. The phrasing of the issue is going to be broken down in great depth in the next part.

$$\xi_{i,j} = t_{i,j} + d_{i,j} + u_{i,j} = 1 \quad (1)$$

Many different sectors of the economy are of the opinion that the integration of information and communication technology with the current transportation infrastructure system and the cars themselves will result in a more contemporary form of travel. The reality of what the industry believes and understands to be possible for a wide range of use cases and applications is made possible by the technology known as VANET. The Vehicle Ad Hoc Network, or VANET, is a self-organizing network that is established by a collection of intelligent cars. When they are within the transmission range, intelligent cars are able to communicate with one another without the need for any permanent infrastructure or centralized

DOI: https://doi.org/10.54216/IJWAC.030105
Received: March 23, 2021 Accepted: August 15, 2021

management. Even if two vehicles are separated by a significant distance from one another, they are still able to communicate with one another via WRSU.

$$SCF_{i,j} = \frac{pf_{i,j}}{pf_{i,j}+pd_{i,j}+pw_{i,j}} \quad (2)$$

The works that have been presented make the assumption that VANET will be deployed with the following qualities in order to carry out effective routing and optimum resource allocation.
It was taken into consideration that the experimental scenario would include a "Vn" number of vehicles/nodes and a "DTn" number of data transmissions/packet forwarding. The Adhoc On-Board Unit (AOBU), the Wired Road Side Unit (WRSU), bandwidth, internal memory, and node energy are all handled as resources in this formulation of the issue.

$$dt_{i,j} = (\omega_1 \times AER_j) + (\omega_2 \times SCF_{i,j}) \quad (3)$$

In the planned works that are covered in proposed works 4, 5, 6, and 7, the experiments have been carried out, and the findings have been examined. The findings are studied in order to demonstrate the relative effectiveness of the works that have been suggested about the efficient routing and resource allocation process employing homogeneous and heterogeneous resource classes. To be more explicit, it's possible that AOBU and WRSU have the same or different configurations for their sensing, communication, and control hardware peripherals, as well as their battery power. Therefore, there are a total of "RTn" resource classes, all of which are either identical or different from one another.

$$\Sigma m(A) \mid A \subseteq \Theta = 1, m(\emptyset) = 0 \quad (4)$$

According to the mobility characteristics of the cars and nodes that make up VANET, all of the vehicles and nodes move in a particular lane in the same general direction (Dhurandher et al. 2010). It is not required to flood the network with data packet broadcasts as it does with conventional wireless networks since the nodes that make up the network are spread out throughout the full area of 360 degrees.

$$B\ \mathrm{Bel}_i(T) = \sum_{A \subseteq T}\ m(A), \forall A \subseteq \Theta \quad (5)$$

Therefore, it is proposed to choose the angular geographical zone that is most suitable for the transmission of data. The data packets are only sent to the nodes that are located between the source and the destination nodes while using this method. The involvement of unneeded nodes in the routing mechanism of VANET is something that is actively being worked to eradicate. This optimum acute angle zone selection approach helps in preserving a lot of the network's resources (WRSU, AOBU), and it also helps in minimizing the total number of control packets created and flooding in the network.

$$m_1 \oplus m_2(T) = \frac{\sum_{A \cap A_{k'}=A} m_i(A_k) m_j(A_{k'})}{\sum_{A \cap A_{k'}=0} m_i(A_k) \cdot m_j(A_{k'})} \quad (6)$$

Additionally, this methodology helps in selecting optimal acute angle zones. In the studies that have been done before, the fundamental concept of the angular zone or geographical region-specific routing systems has already been suggested. However, to the best of our understanding and knowledge, the study works that we have presented are distinct from those works since they include keeping task completion tables, carry stores, and forward tables.

$$u_{i,j} = m_1 \oplus m_2(T) = \frac{\sum_{A \cap A_{k'}=A} [\omega_i m_i(A_k) \cdot \omega_j m_j(A_{k'})]}{\sum_{A \cap A_{k'}=[} [\omega_i m_i(A_k) \cdot \omega_j m_j(A_{k'})]} \quad (7)$$

In each of the four works that have been proposed, it has been assumed that if a vehicle Vi is a source that wants to send a data packet to a vehicle Vj, then the source vehicle/node (Vi) calculates the angular transmission zone by joining the Vi with Vj.

$$\xi_{i,j} = \begin{cases} dt_{i,j}, & \text{if } dt_{i,j} > \alpha \\ dt_{i,j} + rt_{i,j}, & \text{if } \beta \le dt_{i,j} < \alpha \\ 0, & \text{if } dt_{i,j} < \beta \end{cases} \quad (8)$$

In order to carry out this operation, it is necessary to make the assumption that all cars and nodes are equipped with GPS and have the ability to get their own position coordinates as well as those of the destination node.

Algorithm 1: Proposed Work

Input: Set of distinct routing paths (Ω) between the source and the destination

DOI: https://doi.org/10.54216/IJWAC.030105
Received: March 23, 2021 Accepted: August 15, 2021

Output: Trusted path p_n between the source and the destination
1: for each path $p_n \in \Omega$ do
2. Set flag=1
3: for each node $i \in p_n$ do
4: Node i computes $dt_{i,j}$ of next hop j using weighted AER weighted SCF
5: If $dt_{i,j} > \alpha$ then
6: Node i regard node j as 'Trusted'
7: else
8: if $dt_{i,j} \geq \beta$ and $dt_{i,j} < \alpha$ then
9: Node i treats node j as 'Uncertain'
10: Node i computes opinion $\xi_{i,j}$ of node j using direct trust $dt_{i,j}$, and recommended trust $rt_{i,j}$
11: if $\xi_{i,j} \geq \alpha$ then
12. Node i is regarded as a node j as 'Trusted'
13: else
14: Node i regard node j as 'Distrust' and the path p_n is rejected.
15: Set flag $= 0$
16: Break
17: end if
18: else
19: Node i regard node j as 'Distrust' and the path p_n is rejected.
20: Set flag $= 0$
21: Break
22: end if
23: end if
24: end for
25: If flag=1 then
26: Path p_n is 'Trusted'
27: end if
28: end for

The Location-Lookup Table is consulted by the nodes for this purpose (LLT). The information included in the LLT consists of coordinates, velocity, nodes ID, and the angular distance between them. During this stage of the procedure, the sender node will choose an initial angle of 1.

The angle might be anything between 20 and 40 degrees. On both sides of the vector that connects the vehicle/node Vi to the vehicle/node Vj, the resources that are included inside are scanned. The angle is progressively raised by 20 or 30 degrees until it locates the car it is looking for as the destination. According to two studies that were published relatively, there is a possibility of accessing the location of the vehicle even without the use of GPS.

4. Results and Analysis

The BH-AODV is evaluated based on a range of performance criteria, including the average goodput, MAC/PHY overheads, average end-to-end latency, PDR and PLR, along with variations in the number of cars, the length of the simulation, and the speed of the vehicles.

In this part, the vehicle density will be changed in order to study the impact that an assault from a black hole has on a variety of performance characteristics. The number of cars is changed, but the pace of travel is kept constant at 20 meters per second during the whole simulation, which lasts for a predetermined period of 20 seconds. It has been found that the goodput is at its lowest with the lowest vehicle density, which is to say that it is 5.248 kbps for 20 cars. On the other hand, it is at its greatest with the largest vehicle density, which is to say that it is 12.8512 kbps for 120 vehicles. The MAC/PHY overheads study performed on BH-AODV demonstrates that there is a constant rise in overheads with the increase in vehicle density. The delay from beginning to finish increases to 99 milliseconds even for the smallest number of cars, and it reaches an extremely high value of 524 milliseconds for the largest number of vehicles. Because the number of sent packets rises in tandem with the total number of cars, the available bandwidth is continually put to use, which in turn leads to an ever-increasing number of administrative burdens.

DOI: https://doi.org/10.54216/IJWAC.030105
Received: March 23, 2021 Accepted: August 15, 2021

While the number of dropped packets is quite low across the board for all of the simulations run in this part of the article, the number of lost packets is growing as the density of cars increases. The 60 cars scenario results in the greatest possible PDR of 69% and the lowest possible PLR of 28%. Overall, the PDR% is not satisfactory, and even a single black hole assault brings down the performance of the network to such a low level in comparison to that of AODV.

Table 1: Simulation Parameters

No. of Vehicles	Delay (ms)	Transmitted Packets	Received Packets	Drop Packets
20	99.0174	1439	885	5
40	169.351	1633	1034	3
60	425.835	3319	2313	1
80	355.29	2565	1287	1
100	238.788	2217	711	1
120	523.559	4212	2185	1

i. Performance Metrics

In order to evaluate how well our suggested EAER-AODV performs, we have taken into consideration the following four metrics: I Throughput is the number of packets that a destination node manages to receive in a given amount of time. (ii) The Packet Delivery Ratio, also known as PDR, is the ratio of the number of packets received to the total number of packets. (iii) The average end-to-end delay, which is the amount of time that passes between the transmission of a packet and its reception, and (iv) Routing Overhead This is the total number of data packets received divided by the total number of routing packets received.

ii. Simulation Results

The average throughput of EAER-AODV, TDS-AODV, and TAODV is depicted in Figures 1 and 2, respectively, with regard to varying percentages of malicious nodes and speeds. When compared to TDS-AODV, the average routing throughput of EAER-AODV is 49.75% higher, while the throughput of TAODV is only 33.75% higher. According to Figure 3, EAER-AODV has the potential to effectively stop malicious nodes from becoming the next hop in the chain. In this particular experiment, the speed ranges anywhere from 24 to 30 meters per second.

DOI: https://doi.org/10.54216/IJWAC.030105
Received: March 23, 2021 Accepted: August 15, 2021

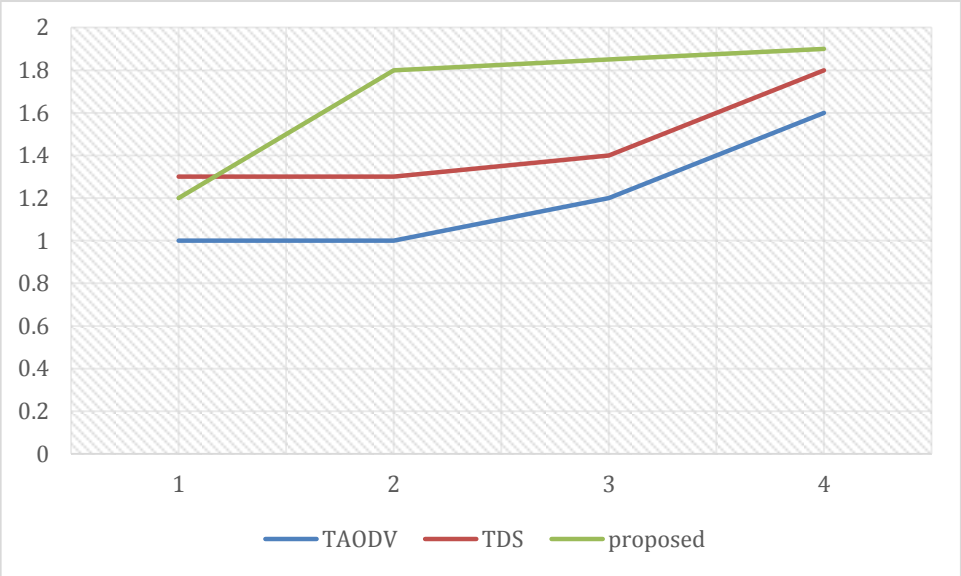

Figure 1: Network throughput with different percentages of malicious nodes

As can be seen in Figure 2, the throughput of EAER initially performs worse than TDS-AODV and TAODV, but as the speed increases, it outperforms both of these algorithms. The reason for this is that nodes with a higher AER value are excluded from becoming the next hop in the chain. The average throughput of EAER-AODV is 22% higher than that of TDS-AODV; however, the throughput of EAER-AODV is 14% lower than that of TAODV due to the fact that it has a lower throughput in scenarios with low mobility. This experiment is carried out with the participation of thirty malicious nodes.

Figure 3 illustrates the packet delivery ratios (PDR) of EAER-AODV, TDS-AODV, and TAODV. The packet delivery ratio of EAER-AODV increases gradually; however, as the number of malicious nodes increases, EAER-AODV demonstrates an improvement over TDS-AODV. When compared to TDS-AODV, the average packet delivery ratio of EAER-AODV is 10.3 percentage points higher, and it is 19 percentage points greater than TAODV. Because of this, only reliable intermediate nodes are chosen to carry packets all the way to their intended destination.

DOI: https://doi.org/10.54216/IJWAC.030105
Received: March 23, 2021 Accepted: August 15, 2021

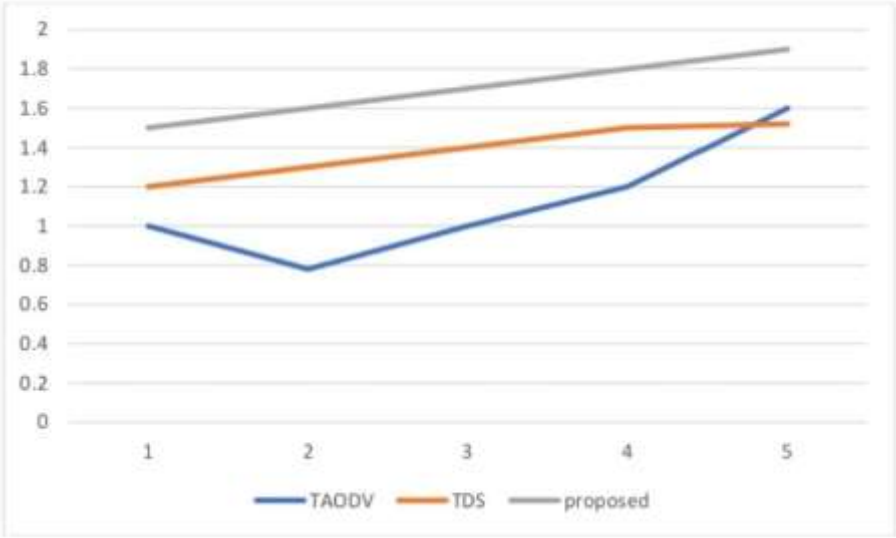

Figure 2: Network throughput at a different speed

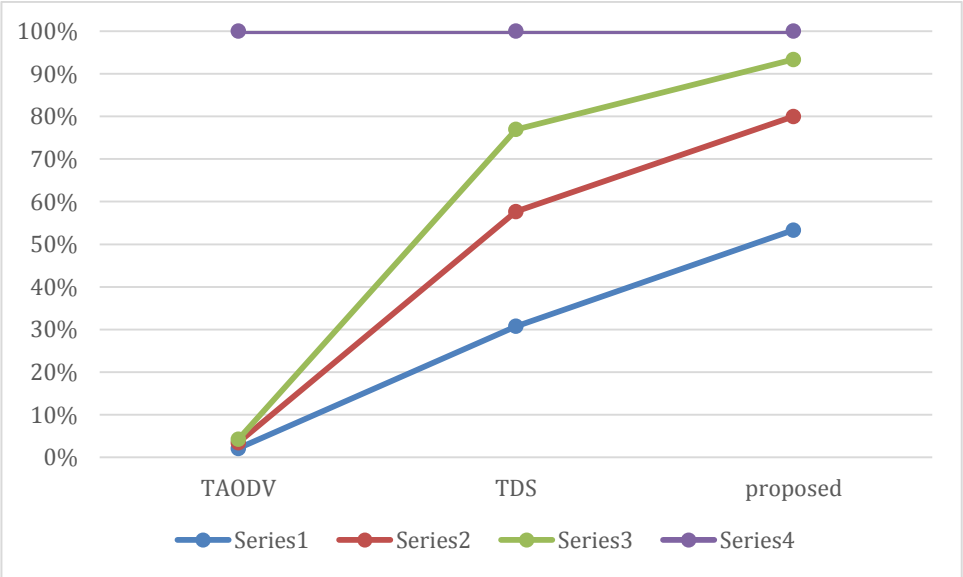

Figure 3: Packet delivery ratio with different percentages of malicious nodes

Figure 3.6 demonstrates that the packet delivery ratio of EAER-AODV is superior to that of TDS-AODV as the speed of the network increases.

DOI: https://doi.org/10.54216/IJWAC.030105
Received: March 23, 2021 Accepted: August 15, 2021

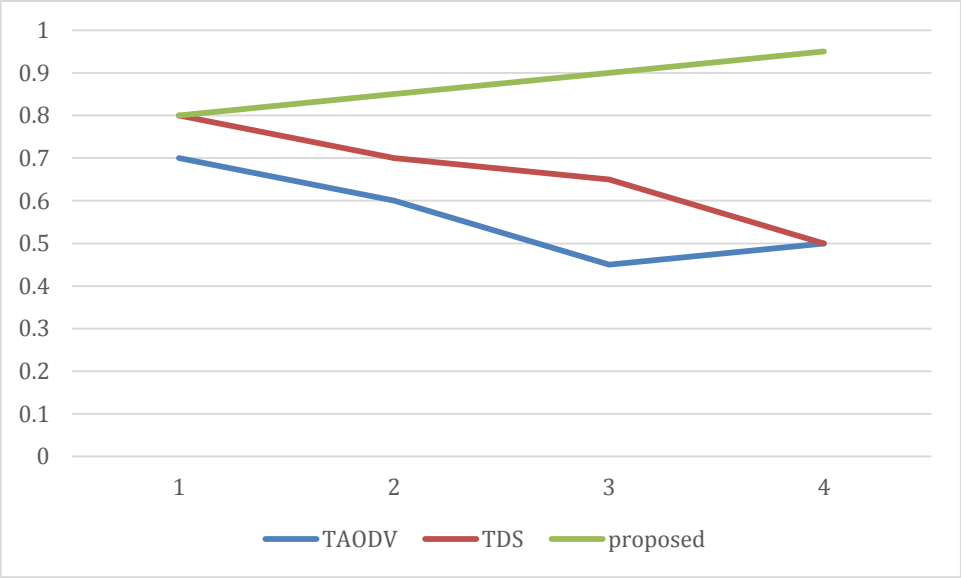

Figure 4: Packet delivery ratio at a different speed

The typical lag time for each of the three approaches is shown in Figure 4, which compares their respective speeds. The maximum speed may be increased, however, this will result in a longer delay. According to these findings, EAER-AODV has effectively captured the dynamic aspect of the topology.

6. Conclusion

Since the proposed work previously knew that the first cluster contains the "Best-customers," defined as those who have made a purchase in the last month (R=1), are frequent buyers (F=1), and spend the most money (M=1), proposed work was able to draw this conclusion. The second activity's customers are more likely to be in the process since their most recent transaction was relatively recent in time (R=4), they purchased fewer products (F=4), and they spent less money (M=4). More efficient programs to help people find permanent jobs inside the organization are needed. It is more probable that the third group is connected to the "Almost Lost" subsection since they have not yet acquired it in the long term (R=3) but have utilized it to acquire and spend a great lot. The last, and most important part of a client base consists of very loyal, high-spending consumers.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Sharma, A., and N. Kumar (2013). Trust Based Theoretical Framework for Mobile AdHoc Networks, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 6, pp. 905-909.
[2] Balakrishnan, V., V. Varadharajan, U. K. Tupakula and P. Lucs (2007). Trust and recommendations in mobile ad hoc networks, in Proc. 3rd International Conference on Networking and Services, pp. 64–69.
[3] Buchegger, S., and J.Y. L. Boudec (2002), Performance Analysis of the CONFIDANT Protocol, in Proc. 3rd ACM international symposium. Mobile Ad Hoc Network. Computing, pp 226–236.
[4] Chen, H., and Z. Ye (2008). Research of P2P Trust based on Fuzzy Decision-making, International Conference on Computer Supported Cooperative Work in Design, pp. 793-796. England,
[5] P., Q. Shi, B. Askwith, Bouhafs (2012). A Survey Of Trust Management In Mobile Ad-Hoc

DOI: https://doi.org/10.54216/IJWAC.030105
Received: March 23, 2021 Accepted: August 15, 2021

Networks, Proceedings of the 13th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking, and Broadcasting.
[6] Eschenauer, L., V. D. Gligor, and J. Baras (2002). On Trust Establishment in Mobile Ad Hoc Networks, Proc. 10th Int'l Security Protocols Workshop, Vol. 2845, pp. 47-66.
[7] De Rango, F., (2009). Improving SAODV Protocol with Trust levels management, IDM and Incentive Cooperation in MANET, Proceedings of the Conference on Wireless Telecommunications Symposium, pp. 352-359.
[8] Qin, F., and Y. Liu (2009). Multipath Routing for Mobile Ad Hoc Network, Proceedings of International Symposium on Information Processing, pp 237-240.
[9] Geetha, S., and G. Geetha Ramani (2014). Survey of Trust-Based Routing Protocols in MANET, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, No. 10, pp. 604-608.
[10] Ghorpade, V.,R.,(2008). Fuzzy Logic based Trust Management Framework for MANET, DSP Journal, Vol 8, No. 1.
[11] Ghorpade, V., R.,Y. V. Joshi and R. R. Manthalkar (2014). Fuzzy Logic based Trust Management Framework for MANET, Journal of Shivaji University (Science & Technology), Vol. 41, No. 1, pp 83-98.
[12] Griffiths, N., K.M. Chao, and M. Younas (2006). Fuzzy trust for peer-to-peer systems, IEEE International Conference on Distributed Computing Systems Workshops, pp. 73-73.
[13] Hallani, H., and A.Hellany (2009). Wireless Ad-hoc Networks: Using Fuzzy Trust Approach to Improve Security between Nodes, In International Conference on Computer Engineering & System, pp. 359-365.
[14] He, Q., D. Wu, and P. Khosla (2004). SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks, in Proc. IEEE Wireless Communications and Networking Conference, pp. 825–830.
[15] Ho, J., W. (2009). Zone-based trust management in sensor networks, IEEE International Conference on Pervasive Computing and Communications, pp. 1–2.
[16] Chen, R., J. Guo, F. Bao and J.H. Cho (2014). Trust management in mobile ad hoc networks for bias minimization and application performance maximization. Ad Hoc Networks, Vol. 19, pp 59-74.
[17] Woungang, I., M. S. Obaidat, S. K. Dhurandher, H. C. Chao and C. Li (2012). TrustEnhanced Message Security Protocol for Mobile Ad Hoc Networks, IEEE International Conference on Communications, pp 988–992.
[18] Sen, J., (2010). A Distributed Trust Management Framework For Detecting Malicious Packet Dropping Nodes In A Mobile Ad Hoc Network, International Journal of Network Security & Its Applications, Vol. 2, No. 4, pp 92-104.
[19] Jiang., J and J. S. Baras (2006). Trust evaluation in anarchy: A case study of autonomous networks, IEEE International Conference on Computer Communications, pp. 1–12.
[20] Cho, J. H., and R. Chen (2013). On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Networks, Elsevier B.V, Vol. 11, No. 8, pp. 2217– 2234.
[21] Josang, A., R. Ismail and C. Boyd (2007). A survey of trust and reputation systems for online service provision, Decision support systems, Vol. 43, pp. 618-644.

DOI: https://doi.org/10.54216/IJWAC.030105
Received: March 23, 2021 Accepted: August 15, 2021