Date of publication SEP-30, 2022, date of current version JUN-14, 2022.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.21.3.2688

A Novel and Enhanced Routing Protocol for Large Scale Disruption Tolerant Mobile Ad hoc Networks

HAMID ALI ABED AL-ASADI[1,2], HUDA A. AHMED[3], ABDUL-HADI AL-HASSANI[1], N A M AHMAD HAMBALI[4]

[1]Communications Engineering Department, University College, Basra, 61004, Iraq.
[2]Computer Science Department, University of Basrah, Basra, 61004, Iraq.
[3]Faculty of Computer Science and Mathematics, University of Kufa, Iraq,
[4]Faculty of Electronic Engineering Technology, Universiti Malaysia Perlis, Kampus Alam UniMAP, Pauh Putra, 02600 Arau, Perlis, Malaysia.

Corresponding author: Hamid Ali Abed Al-Asadi (e-mail: 865.hamid@gmail.com).

ABSTRACT Because of the lack of fixed infrastructures, the existence of open media and diverse network topologies, internetworking networks and mobile ad hoc networks (MANET's), the design of MANET protocols is complicated. In this paper, we propose an evolutionary trust mechanism imitating cognitive processes that uses sensitive information to avoid routing. Moreover, we propose an Enhanced Self-organizing Cooperation and Trust based (ESCT) Protocol, where the mobile nodes share self-reliance and interpret information from a cognitive point of view. Each node develops its information dynamically to eradicate malicious entities. The most attractive attribute of the proposed ESCT protocol, even if domestic attackers know how it operates, is to prevent infringements. In this paper, the efficiency of the proposed ESCT protocol is assessed for different routing disturbances and varying number of attackers. The results of a simulation show that, the proposed ESCT protocol supports diverse network platforms and provides an efficient routing method for MANET routers. The proposed ESCT protocol displays increased throughput, reduction in end-to-end delay and increase in packet delivery ratio when compared to the peers that were taken for comparison.

KEYWORDS MANET; Hole Attacks; Trust Based Routing; Evolutionary; Routing Protocol.

I. INTRODUCTION

MOBILE device usage has driven the evolution of mobile ad hoc networks. These networks are made up of moving node groups which dynamically exchange data without relying on central or fixed base stations (BS). The autonomous function makes it easy for MANETs to be identified in different situations, including rescue, emergency operations and communication in the battlefield [1-3]. However, MANETs unpredictably change mobility and organizational topology. Wireless sensor network (WSN) has specific variations when compared to MANETs [4, 5]. Overall classifications of routing protocols in WSNs and MANETs are depicted in Fig. 1. The wireless networks are mainly classified into infrastructure networks and infrastructure-less networks [6, 7]. MANETs fall under infrastructure-less networks as they are void of any fixed infrastructures [8]. Adhoc network shall be further classified into WSNs, mobile ad hoc networks, vehicular ad hoc networks, wireless mesh networks and flying ad hoc networks [9]. In MANETs, the transfer of data from the closest nodes needs to be supported [10, 11]. Therefore, the enactment of MANETs principally relies on reliable routing of the nodes. In past 10 years, widespread routing literatures with MANETs ended up with several advanced routing protocols [12]. However, the intention is to ensure that every node is entirely self-possessed and prepared to collaborate with all these routing protocols.

As a result, they are vulnerable to attackers who do not cooperate or flout routing rules. Three kinds of routing interruptions are easily caused by MANETs [13]: (1) black holes, (2) passive black holes and (3) gray holes. An attacker continuously claims to possess the shorter route to the destinations when they have active black hole attacks, although they have no correct information on the routes. An active black hole attacker shall call and silently drop large volumes of data packets. Attackers support routing, but all the data packets are discarded in passive black hole attacks. No gray-hole packets have been eliminated for gray-hole attacks. Attackers can selectively transmit the data packets, maximizing their own interests. Gray hole attackers, in other words, are fine and critically behaved.

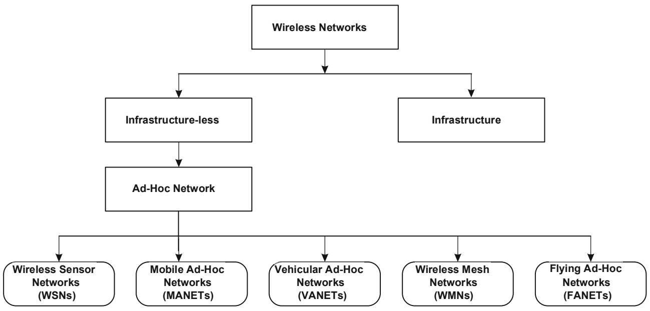
Wireless Networks
Infrastructure-less
Infrastructure
Ad-Hoc Network
Wireless Sensor Networks (WSNs)
Mobile Ad-Hoc Networks (MANETs)
Vehicular Ad-Hoc Networks (VANETs)
Wireless Mesh Networks (WMNs)
Flying Ad-Hoc Networks (FANETs)

Figure 1. Overall classifications of Routing Protocols in WSNs and MANETs.

However, equally the black passive and gray hole attackers are not going to insert redundant network data that means they are passive routing attackers. So as to address these issues, a novel ESCT Protocol which can be considered a value added security mechanism and traditional routing procedures in order to avoid serious negative effects caused by routing disruptive attackers is proposed. As the name indicates, this system has two pillars: every single node carries out self-detection, so that the confidence levels of other nodes (benign or malicious nodes) can be assessed independently. Every node creates more confidence in the exploration of trust information. Each node generates more confidence in its confidence. Moreover, self-detection experiences have an effect on optimistic or pessimistic position of a network node and therefore affect the decision to collect confidential information in the neighbourhood. The proposed ESCT Protocol has the following key elements in comparison with existing preventive routing schemes [14]: researchers are intuitively aware that it is difficult to guarantee the reliable routing of MANET with high mobility. We will show in this paper that mobility can effectively improve the safety. With current routing protocols, we enhance and develop a generic reliability assessment system which can be easily implemented. This proposed ESCT Protocol needs to exchange trust information on a regular basis from direct neighbours. The ultimate confidence of Node Y will however be impaired by not just the number of voting nodes in X's neighbours, but also X's attitude towards the network environment. In comparison to common neighbourhood findings, each node places more confidence in trust information about oneself. In addition, this sensitive information can only be changed if nodes are given new higher or equivalent rights. It shall be examined on different forms of sensitive information and alter the view of the network. It must be emphasized that, the proposed ESCT Protocol is not a complete confidence system capable of accommodating all kinds of MANETs. The only scenarios, such as military exercises, catastrophic rescue and mining, are those free from predefined nodes.

Therefore, within a short time, source nodes would be capable in fulfilling its previous target node(s). The proposed ESCT Protocol is based on a basic viewpoint of mankind – a source node will know if it directly checks the previous destination node. The route is credible or not. The source node could not reach its previous destination node(s) and the proposed ESCT Protocol would not operate correctly in other MANETs, e.g., Ad hoc vehicle networks (VANETs). The proposed ESCT Protocol also requires the legacy and authorization of all network nodes, i.e., ownership of the single authority, to enter into the network. For example, the soldier's name or the rescuer's name provides a node identifier (ID). Finally, the proposed ESCT Protocol aims at the dynamic exchange of package receipts amid source nodes and its target nodes. It results in additional energy use and end-to-end delays, but it supports the networks for defending the routing problems.

This paper is structured as follows. The features and classifications of routing protocols in MANETs and their requirements are elaborated in Section 1. A literature survey of various protocols in MANETs is done in Section 2. The network model encompassing the present research is discussed in Section 3. The operational features of the proposed ESCT Protocol are elaborated in Section 4. The simulation results and discussions are shown in Section 5. Finally, Section 6 gives the conclusion.

II. RELATED WORK

Safe routing is a key element of network performance. Safe and traditional protocols for routing [15] use different tools to ensure accurate network information is not entrusted by active assailants. A detailed review of these protective routing protocols indicates that the network is being worked by a centralised or distributed third party. This implies that, secret keys are already accessible between network nodes. In MANETs, these results are however incorrect. MANETs are as it is known to be different and they fundamentally discard reliance on circumstances, which cannot be predicted. Security operations such as device and authentication of digital signatures are also considered.

Mobile nodes are costly to compute with resource constraints. The main issue with these secure protocols is that passive attacks like passive black hole or gray hole attacks cannot be detected. Therefore, MANETs are a modern way of using efficient routing schemes. Two category groups may in conventional words be classified as a confidence-based routing scheme to minimize the misconstrued or non-cooperative node [16]. Every node uses overheating in most task-driven systems to track the packet transmission status of neighbouring nodes and assesses the status of forwarders based on survey results [17]. In parallel, node monitoring can increase this credibility to improve network trust for pairs [18]. Then nodes with cumulative levels of credibility can be transformed in abstract mathematical specifications.

Finally, each node uses confidence values to differentiate malicious from benevolent nodes. However, there are many issues with these exceptional schemes: (i) nodes must keep on accepting packets that can result in resource loss from their neighbors; (ii) to help each other gain additional network knowledge, the reputation level should be shared among nodes in many popular networks, however, the credibility system is vulnerable to false statements or what other parties consider scores; (iii) false approvals are rendered by internal attackers [19]; (iv) most frameworks of surveillance are not collaborative; (v) overhearing will not be available at all times for every wireless interfaces, e.g., in the asymmetric connection setting.

The credit schemes and game theories form the basis of the second type of cooperative conformity mechanisms. They require sending packets from the source to destination in those systems [20]. Nodes are compensating for the service offered and nodes are compensated for the service received. A credit processing centre specifies the amount of nodes that will be paid or credited for the receipt of received communications. During cooperation, nodes record the required receipt information. If required, credits will be given later. An intimidating framework is also required in addition to the credit processing centre, to guarantee authenticity of the uploaded receipts. These criteria could nevertheless decrease lending system's application in exposed and unplanned networks, including MANETs. In [21-23], game theory was employed in gray hole nodes for the transmission of messages [24, 25]. Nodes with different actions, such as the credit system, play differently [26]. Different players have their own theory kit and often aim to achieve complete benefits by modifying their own tactics.

Finally, a network balance can be developed that prevents players from modifying their payout strategies. But neither credit systems nor game theory systems shall hold the node of maliciousness aimed at reducing network damage [27], like black hole nodes [28], in favour of exploiting their own network advantages. So, to overcome these drawbacks, a new methodology has been proposed and analyzed.

III. NETWORK MODEL

In order to create routes, a network encompassing mobile nodes based on DSR protocol is considered. If the source node contains information, it will trigger road finding by sending a route request (RREQ). If this application has no destination path, or when the route response (RREP) to the source node, including a completed destination route, will continue to broadcast any node receiving the application. Finally, when receiving numerous RREP messages, the source node selects the shortest route for data transmission. When a broken connection is detected during data transmission, the route maintenance will be activated by a route error message (RERR).

If this error message is received by a node, it removes from the route cache the path that contains this broken link. If the data is still passed to source nodes, a new Path Discovery process is started:

- Each node should move freely within a range to allow the source node to reach the previous nodes.
- Each node is identical and learns how it operates.
- Connect with each other via wireless symmetrical connections.
- As decided, by applying laws, to work together before joining, but others have been unconscious since they have joined the network.
- Before joining the network, all nodes must be registered. This means the logging of a contribution to a mobile network connecting a UI to a mobile SIM card. This is commonly considered in the literature if the MANETs only have valid nodes.

The network nodes must be authenticated and use prime security protection to avoid spoofing of the malicious nodes. Therefore, different fake ID protection techniques are considerably based on the authentication mechanisms.

IV. PROPOSED ESCT PROTOCOL

To overcome the shortcomings of the conventional protocols, we propose an ESCT Protocol so that those limitations of contemporary routing systems are resolved in two aspects of the ESCT method including self-detection and mutual-detection.

All nodes perform auto-detection autonomously in the proposed ESCT Protocol, and then transmit the detection results to its immediate neighbours showing decent and malicious peers. After that, each node will conduct cooperative detection to set of additional confidence data for distinguishing malicious node and benign node based on self-detection and information collected from neighbours.

Cooperative detection, in particular, only complements self-detection and never overrides self-detection. Each node transmits messages with a constant frequency to facilitate the functionality of the ESCT protocol. The Sender ID and its updated results are contained here by self-detection. All nodes acquire the IDs of their direct neighbours in suitable manners by exchanging the messages.

This is beneficial when it comes to self-detection. Shared data from the messages help to carry out cooperative detection at the same time.

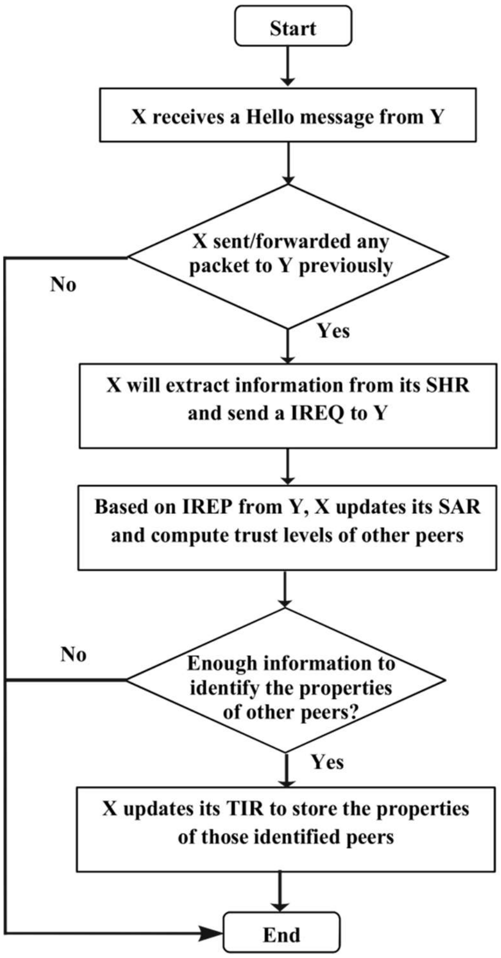
Start
X receives a Hello message from Y
X sent/forwarded any packet to Y previously
No
Yes
X will extract information from its SHR and send a IREQ to Y
Based on IREP from Y, X updates its SAR and compute trust levels of other peers
No
Enough information to identify the properties of other peers?
Yes
X updates its TIR to store the properties of those identified peers
End

Figure 2. Flowchart of Self-detection method in ESCT Protocol.

A. SELF-DETECTION METHOD

The concept of self-detection is basically like human behaviour, where safe way is by direct communication with an individual. For example, only a source or intermediate nodes with the previous target node provides a self-detection mechanism. There are 4-5 MANET connections in a typical link source-to-target.

Preliminary calculations revealed that, if the random route point model takes place at all nodes and max in a 1000 m network area. All nodes' speed is set at a rate of 10 m/s and every node is reached on average not exceeding five times in 2000. As this mode increases these nodes by increasing their power, their maximum speed is increased. Fig. 2 shows the flowchart of self-detection method in the proposed ESCT Protocol.

B. COOPERATIVE DETECTION METHOD

Cooperative detection complements self-detection and contributes secondary rights in cooperative detection to all levels of confidence. When a node receives new information from its neighbours and if enough information has been collected, it may recover and update the value. Fig. 3 describes the procedure of cooperative detection method in ESCT Protocol.

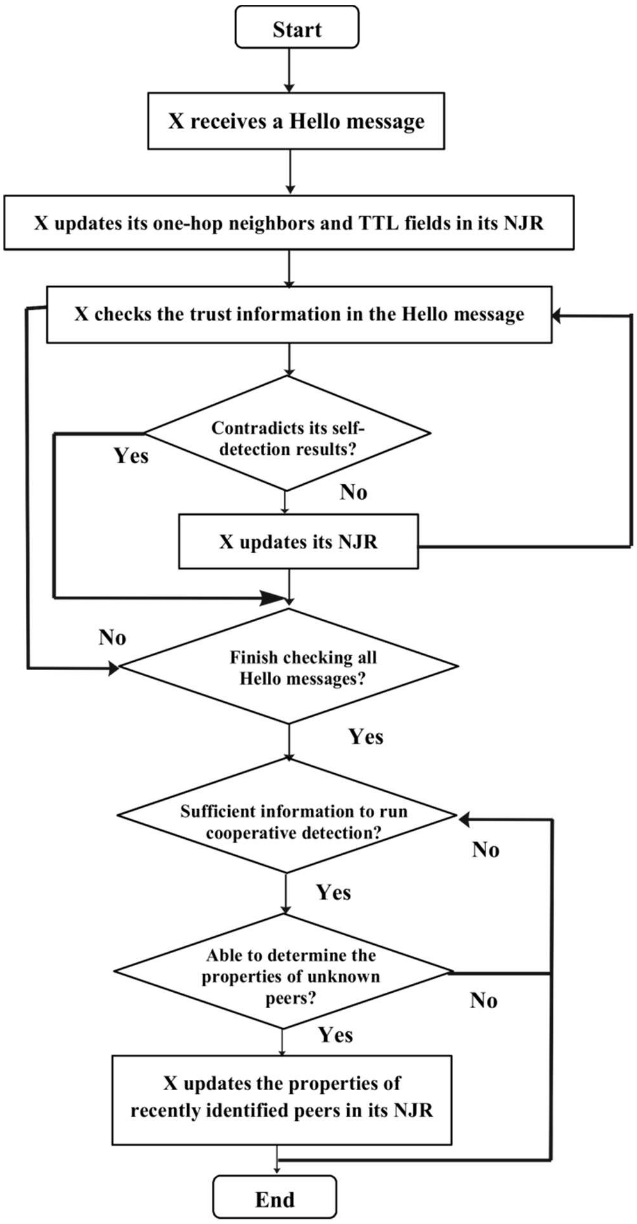
Start
X receives a Hello message
X updates its one-hop neighbors and TTL fields in its NJR
X checks the trust information in the Hello message
Contradicts its self-detection results?
Yes
No
X updates its NJR
No
Finish checking all Hello messages?
Yes
Sufficient information to run cooperative detection?
No
Yes
Able to determine the properties of unknown peers?
No
Yes
X updates the properties of recently identified peers in its NJR
End

Figure 3. Flowchart of cooperative detection method in ESCT Protocol.

V. SIMULATION RESULTS

NS-2 is used for ESCT Performance assessment of the system. DSR is used as the underlying MAC layer IEEE 802.11 routing protocol. Table 1 summarizes the simulation parameters of the proposed ESCT Protocol. The simulated MANET contains 50 nodes that are dispersed uniformly from 1000 m x 1000 m. By default, there are 20 attackers. For node mobility, a random walking model is used.

When simulation starts, each node begins with an altered speed distribution randomly selected between 0m/s and Vmax. Each V max is fixed at 20m/s in the simulation and each node moves to zero when the break is set. The effect of expertise envelopes is also included in this versatility model. A circle of up to 250m as the transmission cover is simulated for each mobile node.

Table 1. Simulation Parameters

Parameter	Value
Area	1000 x 1000 m^2
No. of Nodes	50
No. of Attackers	20
Speed	20 m/s
Coverage	250 m
Packet length	512 Bytes
Simulation time	2000 Seconds
TTL	4 Seconds

There are 10 pairs of flow. A source node CBR rate is fixed, while every 0.25 second a data packet is sent of 512 bytes. Each node has a tail-queue interfaces that contains 20 transmitted packets and each packet is coped in a tail-queue model. Each node begins to exchange Hi messages every second after the simulation starts. The NJR is 4 seconds away from TTL.

Table 2. Packet delivery ratio

Number of Attackers	Protocols	Packet delivery ratio
5	DSDV	0.6
	DSR	0.7
	AODV	0.75
	ESCT	0.9
10	DSDV	0.4
	DSR	0.6
	AODV	0.7
	ESCT	0.85
15	DSDV	0.3
	DSR	0.5
	AODV	0.65
	ESCT	0.8
20	DSDV	0.2
	DSR	0.4
	AODV	0.6
	ESCT	0.7

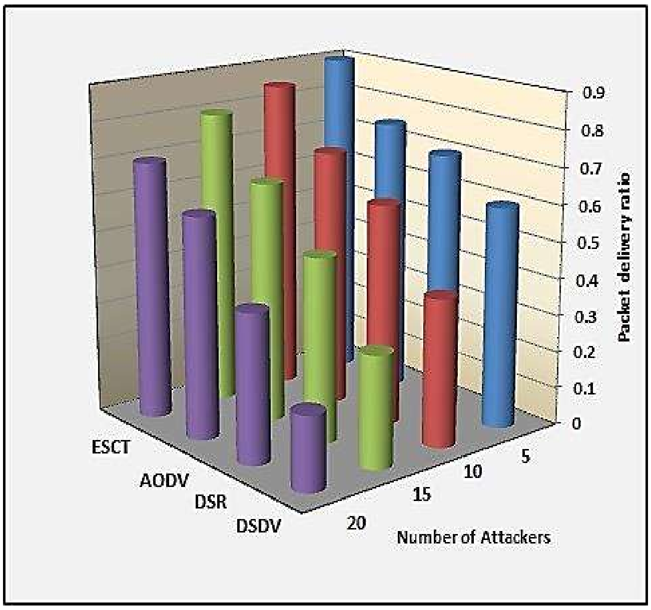

Figure 4. Packet delivery ratio Comparison.

The default is to last 2000 seconds for every simulation run. The α threshold for self-detection is 0.7. As the trust metric of (1), the link between the delivery number and the packet transmission definition is also measured.

The estimated number of data packets and packets transmitted. The packet forwarding ratio above 0.5 and below must be determined by 0.6 for a standard pair. Till 600 source records in SHR and RHR can be included in each node. When the SHR or RHR is finished, automatically it breaks the oldest entry when new messages come in. Every result was demonstrated with 95 percent confidence intervals.

Fig. 4 and Table 2 correspond to the packet delivery ratio corresponding to the number of attackers in case of DSDV, DSR, AODV and proposed ESCT protocol. The packet delivery ratio corresponding to 5, 10, 15, 20 attackers in case of DSDV are 0.6, 0.4, 0.3, 0.2 respectively. The packet delivery ratio analogous to 5, 10, 15, 20 attackers in case of DSR are 0.7, 0.6, 0.5, 0.4 respectively. Similarly, considering 5, 10, 15, 20 attackers towards AODV, the packet delivery ratio are 0.75, 0.7, 0.65, 0.6 respectively. However, the packet delivery to ratio corresponding 5, 10, 15, 20 attackers in case of the proposed ESCT protocol are 0.9, 0.85, 0.8, 0.7 respectively. For this experimentation, the Packet delivery ratio (PDR) shall be assessed by the mathematical expression given below in Equation 1

$$PDR = \frac{\sum No.\ of\ \mathrm{Re}ceived\ \ Packets}{\sum No.\ of\ Packets\ \ Sent}. \tag{1}$$

As per equation (1), the Packet delivery ratio (PDR) is solely dependent on the number of packets transmitted by sender and those received at receiver. In case of the existing DSDV, DSR and AODV protocols, the packet losses during communication are high, thereby their packet delivery ratio are less. The average PDR of DSDV Protocol is 0.375, the average PDR of DSR Protocol is 0.55, the average PDR of AODV Protocol is 0.675, and the average PDR of the proposed ESCT protocol is 0.8125, respectively. As such, the proposed ESCT Protocol exhibits an improvement of 43.75% when compared with DSDV Protocol, an improvement of 26.25% when compared with DSR and an improvement of 13.75% when compared with AODV Protocols.

Hence, it can be suggested that, when packet delivery ratio is a major concern while opting a communication networks, the proposed ESCT Protocol can be selected when compared with the existing DSDV, DSR and AODV Protocols.

Fig. 5 and Table 3 show the variations in throughput with respect to number of attackers in the existing and proposed protocols. Considering DSDV, for number of attackers being taken as 5, 10, 15, 20 the throughput are 72 kbps, 68 kbps, 53 kbps, 51 kbps respectively. For DSR, the throughput is 76 kbps, 73 kbps, 70 kbps, 69 kbps for number of attackers being taken as 5, 10, 15, 20 respectively.

Moreover, in view of AODV, for number of attackers being taken as 5, 10, 15, 20 the throughput are 82 kbps, 77 kbps, 68 kbps, 65 kbps respectively. But, for the proposed ESCT Protocol, the throughput attained by considering 5, 10, 15, 20 attackers are 96 kbps, 92 kbps, 86 kbps, 85 kbps respectively.

Table 3. Throughput (kbps)

Number of Attackers	Protocols	Throughput (kbps)
5	DSDV	72
	DSR	76
	AODV	82
	ESCT	96
10	DSDV	68
	DSR	73
	AODV	77
	ESCT	92
15	DSDV	53
	DSR	70
	AODV	68
	ESCT	86
20	DSDV	51
	DSR	69
	AODV	65
	ESCT	0.7

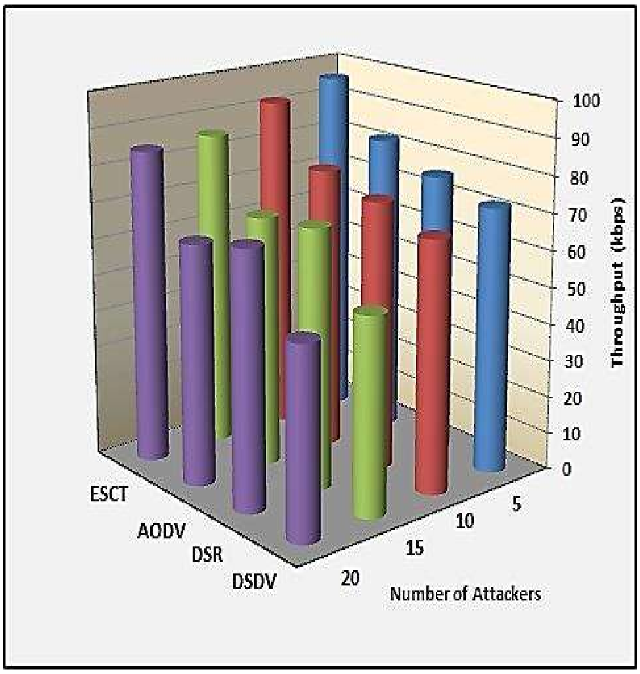

Figure 5. Throughput (kbps) Comparison.

The mathematical representation of throughput used for this experimentation is given below,

$$Throughput\ (T) = \frac{B_{TX}}{\left(t_{END} - t_{START}\right)}. \qquad (2)$$

Throughput represents how the source node transmission gets affected due to the packet losses caused during the transmission. Here, B_{TX} corresponds to overall quantity of packets that are transmitted by the sender node, and (t_{END}-t_{START}) corresponds to the difference between end and start times of data transmission. In this experiment, the average throughput of DSDV is 61 kbps, the average throughput of DSR is 72 kbps, the average throughput of AODV is 73 kbps, and the average throughput of the proposed ESCT Protocol is 89.75 respectively. Accordingly, the proposed ESCT Protocol shows an improvement of 32.03% when compared with DSDV, an improvement of 19.77% when compared with DSR, and an improvement of 18.66% when compared with AODV Protocols. When throughput is a major concern in designing a communication network, the proposed ESCT protocol can be employed at a larger extent.

Table 4. End-to-End delay(s)

Number of Attackers	Protocols	End-to-End delay (s)
5	DSDV	0.16
	DSR	0.15
	AODV	0.15
	ESCT	0.1
10	DSDV	0.18
	DSR	0.16
	AODV	0.16
	ESCT	0.11
15	DSDV	0.18
	DSR	0.15
	AODV	0.15
	ESCT	0.12
20	DSDV	0.18
	DSR	0.17
	AODV	0.17
	ESCT	0.13

Fig. 6 and Table 4 enumerate the comparison of end-to end delay (D) corresponding to variation in the number of attackers of the existing and proposed protocols. By considering DSDV, for number of attackers being picked as 5, 10, 15, 20 the end-to end delay are 0.16 Sec, 0.18 Sec, 0.18 Sec and 0.18 Sec respectively. As such, when the number of attackers is 5, 10, 15 and 20, the DSR Protocol exhibits an end-to-end delay of 0.15 Sec, 0.16 Sec, 0.15 Sec and 0.17 Sec respectively.

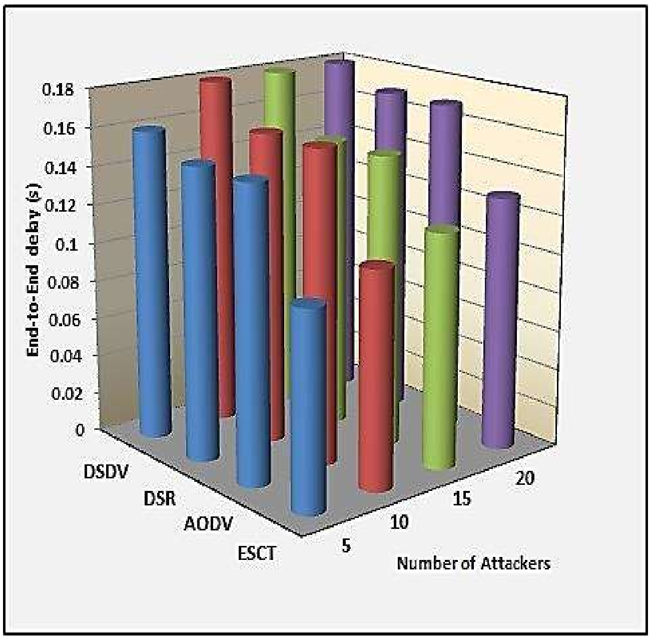

Figure 6. End-to-End delay (s) Comparison.

Furthermore, AODV Protocol corresponding to the number of attackers being 5, 10, 15 and 20, exhibits end-to-end delays of 0.15 Sec, 0.16 Sec, 0.15 Sec and 0.17 Sec respectively. But, the proposed ESCT Protocol exhibits reduced end-to-end delay of 0.1 Sec, 0.11 Sec, 0.12 Sec and 0.13 Sec, when the number of attackers is 5, 10, 15 and 20 respectively. For this experimentation, the end-to-end delay has been assessed by employing the following equation:

$$End\text{-}to\text{-}end\ Delay\ \ D = \frac{\sum_{i=1}^{N_{rec}} D_i}{N_{rec}}, \qquad (3)$$

where, D corresponds to the overall end-to-end delay and N_{rec} corresponds to the quantity of packets that have been received at the receiver node. It is observed that, the average end-to-end delay of DSDV is 0.175 Sec, that of DSR and AODV are 0.1575 Sec, and the average end-to-end delay of the proposed ESCT Protocol is 0.115 Sec.

The proposed ESCT Protocol shows reduced end-to-end delay when compared with the existing protocols, and this is because of the novel features embedded in the proposed algorithm. As such, the proposed ESCT Protocol displays 34.28% reduced end-to-end delay on comparison with DSDV, 26.98% reduced end-to-end delay on comparison with DSR and AODV Protocols. From the simulation results it is clear that ESCT provides better performance and accuracy with different set of cases for different number of attackers.

ESCT relies primarily on the complex interchange of information amid the source nodes and previous target node as it is a direct neighbour. This only happens, however if all nodes, like military applications, are legal and are free to travel. Though ESCT delivery is easily combined with more ad hoc routing protocols, before implementing it in other MANET categories or application-related MANET network patterns, some difficult problems need to be fixed. An auto sensor network needs to be correctly identified, for instance, when nodes are static, as a node can be difficult to locate as it is immediately adjacent to the last target node. The ESCT was designed so that to ensure the correct reception by the use of a multi-path, encryption technique to allow a source and intermediate node for normal IREQ messages transmission. Also, the IREP message to the previous destination node was returned in the same way.

If the storage and processing capacity of the network nodes is heterogeneous, the effectiveness of ESCT is moderate. Finally, at the cost of better standardization and end-to-end latency, the ESCT achieves high PDR and performance. However, in the assailant world there is a marginal end-to-end ESCT delays. Hello messages are used here to preserve the list of adjacent nodes in the largest part of the increased overhead as an unavoidable strategy. The protocols are routed to function correctly.

VI. CONCLUSIONS

MANETs will be commonly used in near future and bring a massive revolution to our lives. However, before effective implementation, it is necessary to solve the safety problem carefully. In this paper, a novel technique is proposed to avoid various routing issues, thereby the proposed ESCT Protocol imitates the human understanding, which in three ways will support the network and improve the output of MANET. First, versatility is used in the self-detection process for trust assessment and it is the basis of the accuracy of the trust assessment. Second, an ESCT cooperation system would increase efficiency and strength. Cooperative identification, on one side, speeds up the measurement of trust and alleviates the lack of expertise. Third, the evolutionary operations in ESCT help nodes to search for different networking styles, to minimize impacts and to correct malicious node self-awareness. The proposed ESCT Protocol depicted increased throughput, lowered end-to-end delay, and better PDR when compared with the existing DSDV, DSR and AODV protocols that were taken for comparison. As a future research, this proposed ESCT method can be evaluated with additional number of attackers in order to additionally validate its effectiveness. Moreover, extra parameters like network overhead, link failure, network scalability, power consumption and packet drop can be considered to evaluate the applicability of the proposed methodology. Additionally, this proposed method can be executed with different node speeds.

References

[1] A. Bujari, L. De Giovanni, C. E. Palazzi, & D. Ronzani, "Location dynamic tabu routing protocol for MANETs," *Mobile Networks and Applications*, vol. 26, pp. 2055–2065, 2021. https://doi.org/10.1007/s11036-021-01744-2.

[2] V. Kulathumani, M. Nakagawa, & A. Arora, "EZ-AG: structure-free data aggregation in MANETs using push-assisted self-repelling random walks," *Journal of Internet Services and Applications*, vol. 9, article number 5, 2018. https://doi.org/10.1186/s13174-018-0077-4.

[3] A. P. Patil, K. Rajanikant, Sabarish, Madan, & Surabi, "Enabling self-organizing behavior in MANETs: An experimental study," In: Satapathy S., Avadhani P., Udgata S., Lakshminarayana S. (eds) ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol I. Advances in Intelligent Systems and Computing, vol 248. Springer, Cham. https://doi.org/10.1007/978-3-319-03107-1_48.

[4] A. K. Gautam, & R. Kumar, "A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks," *SN Applied Sciences*, vol. 3, issue 1, article 50, 2021. https://doi.org/10.1007/s42452-020-04089-9.

[5] M. Carlos-Mancilla, E. López-Mellado, & M. Siller, "Wireless sensor networks formation: approaches and techniques," *Journal of Sensors*, 1–18, 2016. https://doi.org/10.1155/2016/2081902.

[6] S. Shukry, "Stable routing and energy-conserved data transmission over wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, article number 36, 2021. https://doi.org/10.1186/s13638-021-01925-3.

[7] V. K. Quy, V. H. Nam, D. M. Linh, N. T. Ban, & N. D. Han, "A survey of QoS-aware routing protocols for the MANET-WSN convergence scenarios in IoT networks," *Wireless Personal Communications*, vol. 120, issue 1, pp. 49–62. 2021. https://doi.org/10.1007/s11277-021-08433-z.

[8] I. Banerjee, M. Warnier, & F. M. T. Brazier, "Self-organizing topology for energy-efficient ad-hoc communication networks of mobile devices," *Complex Adaptive Systems Modeling*, vol. 8, article number 7, 2020. https://doi.org/10.1186/s40294-020-00073-7.

[9] Y. Fang, X. Zhu, & Y. Zhang, "Securing resource-constrained wireless ad hoc networks," *IEEE Wireless Communications*, vol. 16, issue 2, pp. 24–30, 2009. https://doi.org/10.1109/MWC.2009.4907556.

[10] M. Noura, M. Atiquzzaman, & M. Gaedke, "Interoperability in internet of things: Taxonomies and open challenges," *Mobile Networks and Applications*, vol. 24, pp. 796–809, 2019. https://doi.org/10.1007/s11036-018-1089-9.

[11] C. Ran, S. Yan, L. Huang, & L. Zhang, "An improved AODV routing security algorithm based on blockchain technology in ad hoc network," *EURASIP Journal on Wireless Communications and Networking*, 2021, 1, 2021. https://doi.org/10.1186/s13638-021-01938-y.

[12] M. A. Al-Absi, A. A. Al-Absi, M. Sain, & H. Lee, "Moving ad hoc networks – A comparative study," *Sustainability*, vol. 13, issue 11, 6187, 2021. https://doi.org/10.3390/su13116187.

[13] C. Ran, S. Yan, L. Huang, & L. Zhang, "An improved AODV routing security algorithm based on blockchain technology in ad hoc network," EURASIP Journal on Wireless Communications and Networking, 2021, 1, 2021. https://doi.org/10.1186/s13638-021-01938-y.

[14] M. Shukla, B. K. Joshi, & U. Singh, "Mitigate wormhole attack and blackhole attack using elliptic curve cryptography in MANET," *Wireless Personal Communications*, vol. 121, pp. 503–526, 2021. https://doi.org/10.1007/s11277-021-08647-1.

[15] H. Xu, H. Si, H. Zhang, L. Zhang, Y. Leng, J. Wang, & D. Li, "Trust-based probabilistic broadcast scheme for mobile ad hoc networks," *IEEE Access*, vol. 8, pp. 21380–21392, 2020. https://doi.org/10.1109/ACCESS.2020.2969447.

[16] B. U. I. Khan, F. Anwar, R. F. Olanrewaju, B. R. Pampori, & R. N. Mir, "A game theory-based strategic approach to ensure reliable data transmission with optimized network operations in futuristic mobile adhoc networks," *IEEE Access*, 1–1, 2020. https://doi.org/10.1109/ACCESS.2020.3006043.

[17] R. Skaggs-Schellenberg, N. Wang, & D. Wright, "Performance evaluation and analysis of proactive and reactive MANET protocols at varied speeds," *Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, 2020, pp. 1-5. https://doi.org/10.1109/CCWC47524.2020.9031233.

[18] X. Zhang, C. Lyu, Z. Shi, D. Li, N. N. Xiong, & C. Chi, "Reliable multiservice delivery in fog-enabled VANETs: Integrated misbehavior detection and tolerance," *IEEE Access*, vol. 7, pp. 95762-95778, 2019. https://doi.org/10.1109/ACCESS.2019.2928365.

[19] M. Karthigha, L. Latha, & K. Sripriyan, "A comprehensive survey of routing attacks in wireless mobile ad hoc networks," *Proceedings of the 2020 International Conference on Inventive Computation Technologies (ICICT)*, 2020, pp. 396-402, https://doi.org/10.1109/ICICT48043.2020.9112588.

[20] M. Mohamed Musthafa, K. Vanitha, A. M. J. M. Zubair Rahman, & K. Anitha, "An efficient approach to identify selfish node in MANET," *Proceedings of the 2020 International Conference on Computer Communication and Informatics (ICCCI)*, 2020, pp. 1-3. https://doi.org/10.1109/ICCCI48352.2020.9104076.

[21] T. Chen, L. Wu, F. Wu, & S. Zhong, "Stimulating cooperation in vehicular ad hoc networks: A coalitional game theoretic approach," *IEEE Transactions on Vehicular Technology*, vol. 60, issue 2, pp. 566–579, 2011. https://doi.org/10.1109/TVT.2010.2093587.

[22] S. Daud, S. M. M. Gilani, M. S. Riaz, & A. Kabir, "DSDV and AODV protocols performance in internet of things environment," *Proceedings of the 2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, 2019, pp. 466-470. https://doi.org/10.1109/ICCSN.2019.8905256.

[23] S. Behera, & G. Das, "Dynamic routing and spectrum allocation in elastic optical networks with minimal disruption," *Proceedings of the 2020 National Conference on Communications (NCC)*, 2020, pp. 1-5. https://doi.org/10.1109/NCC48643.2020.9056071

[24] A. Ilavendhan, & K. Saruladha, "Comparative study of game theoretic approaches to mitigate network layer attacks in VANETs," *ICT Express*, vol. 4, issue 1, pp. 46–50, 2018. https://doi.org/10.1016/j.icte.2017.12.002.

[25] R. F. Olanrewaju, B. ul Islam Khan, F. Anwar, R. N. Mir, M. Yaacob, & T. Mehraj, "Bayesian signaling game based efficient security model for MANETs," *Advances in Biochemical Engineering/Biotechnology, Lecture Notes in Networks and Systems series*, Publisher: Springer, Cham, pp. 1106–1122, 2019. https://doi.org/10.1007/978-3-030-12385-7_75.

[26] L. Guaya-Delgado, E. Pallarès-Segarra, A. M. Mezher, & J. Forné, "A novel dynamic reputation-based source routing protocol for mobile ad hoc networks," *EURASIP Journal on Wireless Communications and Networking*, 2019, 1, 2019. https://doi.org/10.1186/s13638-019-1375-7.

[27] A. A. Mahamune, & M. M. Chandane, "An efficient trust-based routing scheme against malicious communication in MANET," *International Journal of Wireless Information Networks*, vol. 28, issue 3, pp. 344–361, 2021. https://doi.org/10.1007/s10776-021-00523-w.

[28] V. S. Janani, & M. S. K. Manikandan, "Efficient trust management with Bayesian-Evidence theorem to secure public key infrastructure-based mobile ad hoc networks," *EURASIP Journal on Wireless Communications and Networking*, 2018, Article number: 25, 2018. https://doi.org/10.1186/s13638-017-1001-5.

***HAMID ALI ABED AL-ASADI** received the B.Sc and M.S. degrees in electrical engineering and communication engineering from Basra University, Basra, Iraq, in 1987 and 1994, respectively, and the Ph.D. degree from the University Putra Malaysia in Communication Network Engineering in 2011. From 1995-2018, he was a faculty member in the Department of Computer science, Basra University. In 2014, he joined the Basra University as a Full Professor. Since November 2018 he has been head of the Department of communication engineering in the Iraq University College, Iraq. His research interests include optical communications, optical fiber, information theory, Wireless Network, Sensor Network, Fuzzy Logic and Neural Networks, Swarm Intelligence, computer engineering, and Artificial intelligence. He is member of scientific and reviewing committees of many journals and international conferences in the domains of Computer and communications engineering.*

***HUDA A. AHMED** received B.Sc and M.Sc. degree in Computer Science from Basrah University, Basrah, Iraq, in 1997 and 2001 respectively. Now a Ph.D. student in Computer Science department, Faculty of Computer Science and Mathematics, Kufa University, Najaf, Iraq. Lecturer with Computer Science Departments, College of Computer Science and Information Technology, Basrah University. Her interesting field on soft computing, neural networks, image processing, and recently Wireless Sensor Networks.*

***ABDUL-HADI AL-HASSANI** received the bachelor's degree from the University of Basra, Basrah, Iraq, the master's degree from the University of Bradford, Bradford, U.K., and the Ph.D. degree from Loughborough University, Loughborough, U.K., He is currently the General Director of the Basra Centre for Strategic Studies and also the Chancellor of the Iraq University College Basrah, Basrah. His research interests include environmental monitoring and applications in construction and disaster prevention.*

***Nor AZURA MALINL BT AHMAD HAMBALI** received her Bachelor's degree in Computer and Communication System Engineering at Universiti Putra Malaysia. She received the degree on 17th August 2000. After graduation she worked as tutor (Information Technology). From November 2002, she continued study in Communication and Network Engineering for Master's degree. After receiving Master's degree, she had been working as a lecturer at MSU (Management and Science University) for 2 years. From 2007, she had been pursuing a study leading to the award of degree of Doctor of Philosophy also in Communication and Network engineering, majoring in Optical fiber laser at Universiti Putra Malaysia and graduated. She is currently a Senior lecturer at University Malaysia Perlis. Dr Nor Azura Malini has also published more than 120 journals/proceedings and book chapter. Professionally, Dr. Nor Azura Malini is also a member of the Institute of Electrical and Electronics Engineers (IEEE), Institution of Engineering and Technology (MIET) and Board of Engineers Malaysia (BEM).*