

Secure Opportunistic Routing Protocol in VANETs

Eqbal Darraji¹, Iain Phillips² ^a and Asma Adnane²

¹Department of Computing, Mustansiriyah University, Iraq

²Department of Computing, Loughborough University, U.K.

Eqbal.darraji@uomustansiriyah.edu.iq, {i.w.phillips, a.adnane}@lboro.ac.uk

Keywords: Security, Trust, Opportunistic Routing, VANETs.


Abstract: In this paper, we introduce a new trusted opportunistic routing protocol called Trusted Context-aware Opportunistic Routing (TCOR) which produces a secured routing for VANET and it is incorporated with a recommendation mechanism (TCOR-Rec). The proposed secure routing protocol aims to address the inherent limitations in VANET routing, particularly the challenges associated with mobility metrics and the incorporation of trust metrics. By leveraging a comprehensive trust framework that integrates both direct and indirect observation-based reputation systems, the protocol enhances the robustness and reliability of the routing process. In addition, a similarity-based evaluation method is employed to assess the validity of recommendation messages, facilitating the selection of the most trusted and reliable path. OMNET++ is used to implement and simulate TCOR, which has proved its efficiency in comparison with other routing protocols (COR opportunistic protocol, AODV and trusted AODV). To simulate an adequate VANET environment and evaluate the protocols under realistic conditions, different metrics and network parameters such as the network traffic pattern, mobility pattern, and the fading propagation model have been used. The results have shown that TCOR and TCOR-Rec outperform traditional routing protocols by approximately 9% and 15%, respectively, in terms of packet delivery when the attacker nodes are involved in the network.

1 INTRODUCTION

Secure routing in wireless communications has been considered a challenging task, particularly in Mobile Ad hoc Network (MANET) due to its characteristics such as limited resources, open medium, and distributed cooperation (Chandramouli et al., 2018). Although applying cryptography and authentication mechanisms achieves security that provides integrity and confidentiality, it is impractical to implement them in Ad hoc networks since it does not solve the issue of cooperation and internal attacks. In recent years, many researchers have been redirected to achieve MANET routing security based on trust approaches to detect internal attacks and motivate nodes to cooperate (Smriti Jain, 2017). Comparison studies of cryptographic and trust-based mechanisms used in secure routing protocols show that the former requires more computation overhead (Kumar and Banerjee, 2017) and (Jhanjhi et al., 2022). In general, the necessity of trust appears only in an environment with uncertainty characteristic, such as e-commerce. In wireless communications, this feature is dominant among

network nodes due to their inability to collect information about nodes that are outside their sensing range. There are many reasons that motivate the use of reputation and trust-based systems as a security solution for wireless networks, for example, individuality of the node in MANETs, the lowest cost of producing nodes in WSNs and cryptography failure in the face of internal attacks (Luo and Lu, 2008).

In MANETs, there is no centralised control, and, as a result, nodes are responsible for performing all network operations. Since there is no shared attentions and individuality of nodes, these nodes may prefer to not cooperate. This misbehaviour (non-cooperation) is either for selfish goals such as to save resources, or malicious ones, for instance, denial of services. Vehicular ad hoc networks (VANETs) are a subset of traditional MANETs in which nodes are mobile and cooperate with each other to route and relay packets. However, these nodes act independently without central network management support, increasing their chance of being malicious, leading to high risks to safety applications. The importance of routing in VANET and MANET environments for the successful delivery of data packets and efficient sup-

^a  <https://orcid.org/0000-0001-8503-7651>

port for applications make security for routing protocols the first crucial step to support VANET applications' security.

2 RELATED WORK

In opportunistic routing (OR) protocols, there are relatively few studies in the area that suggest trust models to improve the reliability of communication and achieve security.

Wu et al. (Wu et al., 2017) proposed a Trust-based Routing Protocol (TRP) to mitigate the impact of malicious nodes in opportunistic networks. The protocol addresses black hole attacks by monitoring previous hop behavior and updating trust values, minimizing the influence of older transactions. Recommendations are based on direct trust from the recommending node, but periodically exchanging opinions from multiple nodes could improve the effectiveness of the protocol. Bo et al. (Bo et al., 2011) suggested an opportunistic routing protocol for MANETs. Hybrid observation (direct and indirect trust) is used to compute the trust on the forwarding node. The cost of the trusted route is calculated according to the node's proximity to the destination and its trust value. In addition, the formulation of a trusted minimum-cost routing algorithm (MCOR) is formally produced. The same idea of MCOR was applied by Zhizhong et al. (Zhizhong et al., 2012) to secure routing in VANETs and devised Trust opportunity forwarding mechanism (TMCOR). Zhizhong et al. (Zhizhong et al., 2013) proposed a protocol where each node evaluates the trustworthiness of its neighbors based on collected data. Trusted neighbors are ranked by routing cost, trust value, and distance to the destination to prevent black-hole and grey-hole attacks. The protocol was compared to the EXoR protocol (Biswas and Morris, 2004), which relies on link quality and distance metrics. However, comparing with an untrusted protocol like EXoR may not accurately reflect real performance, particularly in terms of throughput and packet delivery ratio.

Chuanhe et al. (Huangchuanhe, 2010) introduced the Trust Opportunistic Routing (TOR) protocol, combining expected transmission count (ETX) and trust metrics. ETX estimates link quality via probe packets, while trust is based on the ratio of received to forwarded messages. Candidates are selected for the highest trust and lowest transmission count, with RTS/CTS packets for coordination. TOR excludes malicious nodes and is compared to the ExOR protocol (Biswas and Morris, 2004). Li and Das (Li and Das, 2013) developed a comprehensive

trust model to predict node behaviour, using positive feedback messages as evidence of forwarding behaviour. Trust and message delivery ability inform forwarding decisions, with comparisons made with the Prophet protocol. Elakkiya et al. (Elakkiya et al., 2014) aimed to assess the information obtained, relying on trust metrics and speed for the selection of opportunistic hops. Direct information is collected based on immediate acknowledgements, while recommendations are evaluated using a proposed formula. Trusted Prophet (T-prophet) and AODV protocols were used for evaluation.

Salehi and Boukerche (Salehi and Boukerche, 2014) proposed combining trust and link delivery probability into a single metric to enhance wireless network security. Candidate nodes are selected based on this metric, with a watchdog mechanism for monitoring direct neighbors. Source nodes update trust values and detect misbehaving nodes by monitoring candidate behavior, while time-based coordination among candidates is utilized. An extension of this work (Salehi et al., 2015) introduced a trust model that incorporates geographical location, link quality, and trust value as local metrics for hop selection, aiming at a balanced selection that prioritises historical data. The reputation model proposed in (Salehi and Boukerche, 2014) was extended to incorporate recommendations from other nodes in evaluating trust values (Salehi and Boukerche, 2015). The observation mechanism relies on ideal coordination among the candidate nodes, where each node receives an acknowledgement message when the candidate forwarder transmits the packet and when the sender receives this acknowledgement.

Thorat et al. (Thorat and Kulkarni, 2015) propose a trust mechanism for the CORMAN opportunistic routing protocol, relying on first-hand observation. The top two candidates are selected by evaluating all intermediate nodes toward the destination, using global information to calculate a metric that combines trust value and node proximity. Node reliability is assessed using Bayesian derivation through promiscuous packet forwarding monitoring, while ETX evaluates the node's closeness to the destination.

3 TRUSTED CONTEXT-AWARE OPPORTUNISTIC ROUTING

Trusted Context-aware Opportunistic Routing (TCOR) is based on the previously suggested Context-aware Opportunistic Routing (COR) (Zhao et al., 2014a) (Zhao et al., 2014b). To enhance the security of routing and stop malicious attacks, a trust

mechanism has been incorporated into opportunistic routing to produce TCOR. TCOR uses the trust metric in addition to the other context metrics such as link quality, geographical location, and mobility to make the routing decision. Trusted-Clear-To-Broadcast (TCOR) follows the same steps as COR with Data packets broadcast, trusted-CTB packet generation, Trust-based Next-hop selection, and extra elements added to the design.

The following steps are the key modules of the TCOR protocol.

- **Data Packet Broadcast:**

In this step, the source node starts broadcasting a data packet when it is needed, location and the destination are included. When a neighbour receives this packet, it will calculate the DFD, include it in the CTB packet and reply immediately (which will be called Trusted CTB "TCTB" in TCOR). The source node will set a timer, which is called a CTB timer, in order to get as many CTB packets as possible from all the neighbours.

- **Trusted CTB Packet Generation:**

A Trusted Clear-To-Broadcast (TCTB) control packet is generated by the neighbour that receives the broadcast data packet. Each neighbour receiving a data packet from a source node will immediately reply with a TCTB packet without setting a DFD timer, the TCTB includes the DFD value. At the source node, all the TCTB packets received within the CTB timer period will be saved in a list (TCTB senders list) in order to select the best next hop among TCTB senders after CTB timer expires. This process will be repeated by each intermediate node that is selected as the best candidate (best next hop) until getting the generated TCTB packet by the destination. The DFD is calculated very similarly to COR protocol but the energy parameter was excluded due to no limitations on energy consumption in VANET. The following equation explains how the DFD is computed:

$$DFD = (\alpha \times LinkQuality + \beta \times Progress + \delta \times LIVE) \times DFD_{Max} \quad (1)$$

- **Trust-Based Next Hop Selection:**

When the CTB timer expires, the source node will select the best candidate from its TCTB senders list, in terms of trust and quality of services, as the next hop forwarder. The TCTB sender that has the highest trust value will be selected as the best next hop. When multiple TCTB senders have the same trust value, the one with the lowest DFD value will be selected as the best next hop.

- **Tear Down Timer:**

A tear-down timer is used to maintain the stabil-

ity of connections for the selected route and select the more trusted route after a certain period. The value of this period/timer can be determined based on the network status (e.g. network congestion and nodes' mobility). This timer plays a very important role in establishing a reliable and trusted route as it helps a node rediscover a route after a certain time based on trust and other context parameters, such as link quality, progress, and mobility. This timer will be started for each destination, and when it expires, the (intermediate) node will tear down all the information that has about this destination: route, next-hop trust value and other related buffers. Figure 1 describes the process steps of Tear down timer.

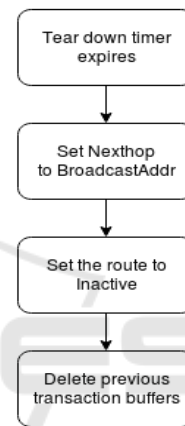


Figure 1: Process steps of Tear down timer.

To accelerate the setup process of the trust system, the first-hand trust information shared with other network nodes periodically and according to a condition to avoid overhead communication and time delay. The period of information sharing is selected based on the CTB timer and updating the trust value. However, this approach exposes the system to false report attacks, making effective mitigation measures essential. A common method to evaluate the trustworthiness of a recommending node is similarity (Bo et al., 2011; Zhizhong et al., 2013), which measures the alignment of opinions and recommendations from multiple nodes regarding the observed node.

4 SIMULATION SETTINGS

In this section, we will introduce the simulation details, as well as Trusted AODV (TAODV) which we used as a comparison protocol with our proposed trust routing TCOR.

4.1 Trusted AODV Routing

TAODV Routing Protocol was proposed by Kamel et al. (Kamel et al., 2017) to detect black hole attack. This trusted routing protocol uses the destination sequence number to detect the malicious node as the attacker node tries to attract the source node by sending a fake RREP message. The proposed mechanism examined the safety status for each RREP message received. Figure 2 illustrates the steps of the RREP process.

Each participating node in the network has a trust level (TL) and malicious node tables (MN). TL determines the level of trust for each node that participates in the network routing activities. All participating nodes are at a trusted level in the initial stage exactly 60. This level is updated during the simulation on the basis of the safety status for each incoming RREP message. To verify the validity of the incoming RREP and its safety status, a threshold needs to be defined. The threshold is calculated using formula 2.

$$Th = \frac{1}{N} \sum_{i=1}^N (rpSeqNo_{pi} - rtSeqNo_{pi}) \quad (2)$$

Where N is the number of nodes in the routing table of node (p). $rpSeqNo$ is the dst_sq_no of the destination node (i), $rtSeqNo$ is the current sequence number for destination node (i) in the routing table of node (p).

In the AODV routing mechanism, routes are selected based on the sequence number and hop count to the destination. Upon receiving an RREP message, the MN table is checked. If the originator node is listed, the message is discarded; otherwise, its safety status is evaluated using the formula 4 (Kamel et al., 2017).

$$\Delta Seq = rpSeqNo_{pi} - rtSeqNo_{pi} \quad (3)$$

$$S = \Delta Seq - \alpha \times Th \quad (4)$$

Here α is the distance from the threshold that secures the information. Based on the value S calculated using formula 4, the incoming information will be defined as safe or unsafe according to formula 5 (Kamel et al., 2017):

$$SecurityStatus = \begin{cases} \text{If } S \leq 0 & \text{Safe RREP} \\ \text{If } S > 0 & \text{unsafe RREP} \end{cases} \quad (5)$$

When an unsafe RREP message is detected, the TL of the originating node will decrease by one. The originating node will be inserted in the MT table when its TL becomes negative.

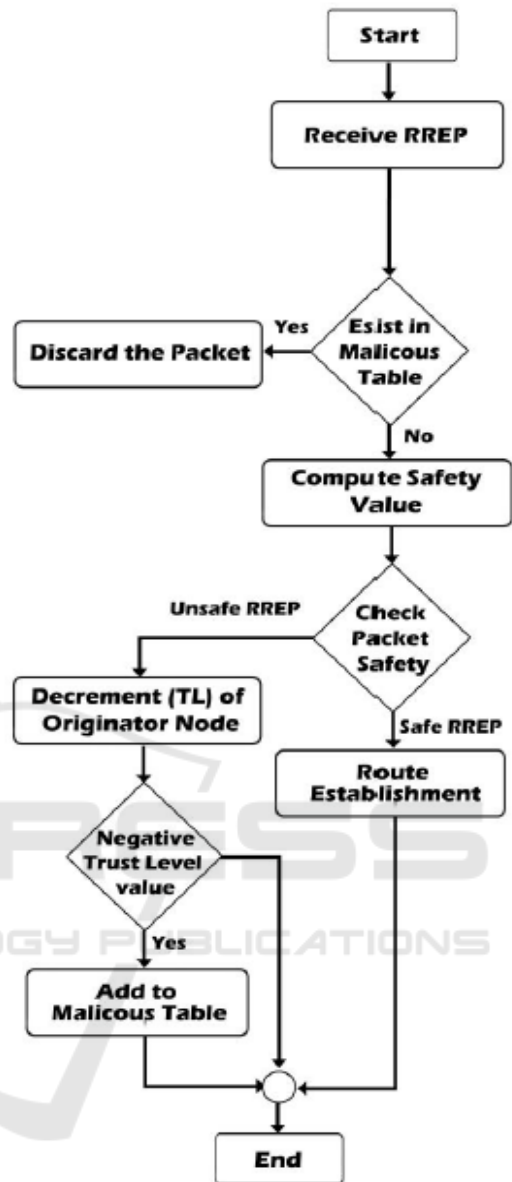


Figure 2: RREP process steps of Trusted AODV (Kamel et al., 2017).

4.2 Attacks Simulation

To evaluate the proposed trusted routing protocol, misbehaving / attacker nodes must be added to the network. There are many attackers that perpetrate the network layer; however, only the most popular attacks were implemented and taken part in the network: Black hole and grey hole attacks. The attacks were implemented in a sophisticated way, where the attacker nodes behave normally in terms of route discovery (exchanging control packets), for instance in COR and AODV, they will reply with CTB and RREP,

respectively, in order to take part in the established path. However, when they are involved in a selected routing path, they will drop all data packets that pass through them. The grey hole attack was carried out to drop 50 % of the data packets in a fluctuating manner. Thus, the attacker nodes have the opportunity to be selected as a router in order to be able to execute the attack.

4.3 Simulation Environment

VEINS 4.5 platform has been utilised to configure simulation experiments. This simulator emulates the VANET environment by coupling OMNeT++ 5.0 (Varga and Hornig, 2008) and SUMO (Ben Mussa et al., 2016) (DLR - Institute of Transportation Systems, 2015) to configure network simulation and road traffic. The mobility model for the used map (Manhattan map) is generated using SUMO with a maximum speed limit of 14m/s. The packet delivery ratio (PDR) and the end-to-end delay (e2edelay) (Zhao et al., 2014a) are the metrics that were used to evaluate the proposed protocol. PDR presents the relationship between the data packets delivered to the destination application layer and the data packets transmitted by sources. However, e2edelay presents the time taken by the transmitted data packet from the source to the destination.

5 PERFORMANCE EVALUATION

The results of the simulation experiments that were carried out with the routing protocols in an urban environment (Manhattan map $750 \times 750m^2$) were evaluated based on PDR and e2edelay. These experiments were run ten times with 100 nodes randomly deployed in the network, and each experiment took 120 seconds to run. Multiple loads (10, 20 and 50 connections) were tested, and these connections (source and destination) were chosen randomly using the same seed number on each run. An interval of each connection was selected in a random manner that differs between 5 and 25 seconds for 10 pps of load 100 bytes to simulate the critical safety application. Figure 3 illustrates the PDR of routing protocols with different load networks.

In Figure 3, the COR and TCOR protocols achieve the highest probability of data packet delivery, especially when the number of connections increases and reaches approximately 13% higher than the traditional routing protocols (AODV and TAODV). This is due to the opportunistic feature of these routing protocols (which confirms the motiva-

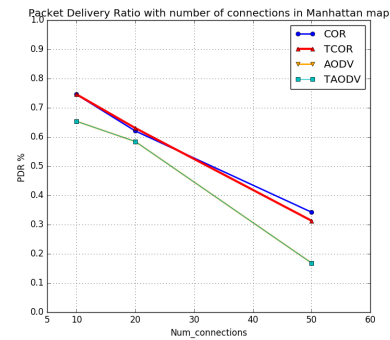


Figure 3: PDR of COR, AODV, TCOR and TAODV in Manhattan map (100 nodes).

tion of this research study (Biswas and Morris, 2004; Wang et al., 2012; Boukerche, 2009) to establish a path (as the path is established when data packets move) and to use multiple contexts of information to make a route decision. In AODV, the path is established before the start of sending data packets (sending RREQ and waiting for RREP), which increases the number of dropped packets in the network layer due to the queue fullness and unavailability of routes. TAODV performs the same way as AODV does, since the modifications cannot affect its performance without attacks.

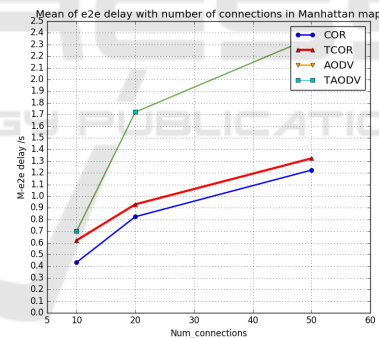


Figure 4: Average of e2edelay with number of connections without attacks.

Figure 4 illustrates the mean of e2edelay for each tested routing protocol with multiple loads. The mean of e2edelay was calculated for each run of the experiment, and then the average was computed for all the runs. As shown in that figure with AODV, the packets take longer to be delivered in various scenarios (10, 20, and 50 connections). This is due to the route initialisation process that starts route discovery (start broadcasting a RREQ message and wait until the RREP message is received) to establish a path to the destination. As TAODV performs the same way as AODV without attacks, it consumes the same time delivering the packets. COR shows

the shortest e2edelay due to its dependence on multiple forwarders (multiple next hop) and uses multiple items of context of information to select the next hop. TCOR and COR are different because TCOR sets a CTB timer to receive multiple replies from the sender’s neighbours. In general, COR and TCOR outperform AODV and TAODV in terms of the packet delivery ratio and the time it takes to deliver the packets to the destination. The routing protocol performance results are analysed and discussed when the network is under black hole or grey hole attacks.

- The performance of AODV significantly declines in terms of packet delivery ratio (PDR) as the number of black hole attacks and network connections increases. The drop in AODV performance is due to its discovery process and its mechanism to establish a path and not incorporating any trust algorithm.
- TCOR outperforms the other routing protocols tested in PDR and e2edelay as seen in figures 5, 6, 7, 11, 12 and 13. It performs better than the other tested routing protocols by approximately 10%, particularly when the number of connections is equivalent to 50 pairs. This is due to its mechanism relying on the trust metric along with contextual parameters, such as mobility, geographic location, and link quality, to make the routing decision. It also achieves the shortest e2edelay as it selects the more trusted neighbour and the closest one to the destination as a next hop (forwarder).
- TCOR incorporating recommendations (TCOR-Rec) improves TCOR performance in terms of PDR, as it helps the network nodes share their experiences (direct trust) with their neighbours during the path establishment without any further exchange messages (as the recommendations were included in the control packets that are used to discover a route). That improvement increases by about 5% in the scenario where 50 pairs of connections are exchanging data. In TCOR-Rec, there is a slight increase in e2edelay compared to TCOR because TCOR-Rec increases the number of candidates’ neighbours, and thus it will be more likely to select the more trusted neighbour even though it is not the closest one.
- TCOR defences against the black hole attacks by detecting and excluding them from taking part in the path establishment, and this is clear through the increased amount in the PDR in comparison with COR in all different urban scenarios (10, 20 and 50 connections) as illustrated in figures: 5, 6 and 7.

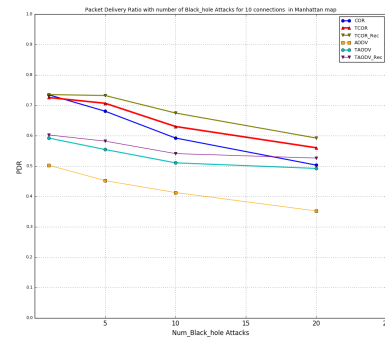


Figure 5: PDR of 10 connections with different number of black hole attacks in Manhattan map.

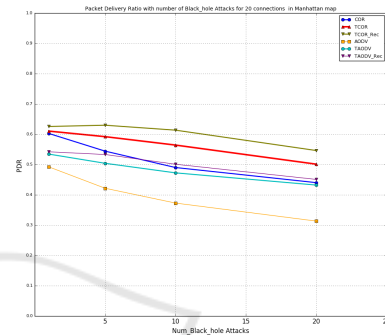


Figure 6: PDR of 20 connections with different number of black hole attacks in Manhattan map.

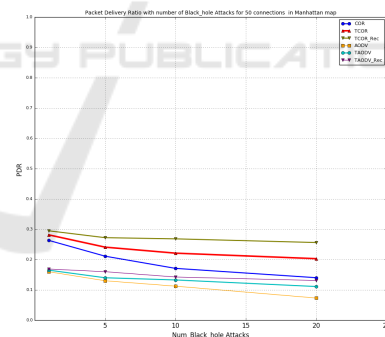


Figure 7: PDR of 50 connections with different number of black hole attacks in Manhattan map.

6 CONCLUSIONS

The results show that the proposed trusted opportunistic routing protocol (TCOR), which incorporates trust and recommendations, outperforms COR, AODV, and TAODV. By integrating trust and recommendation metrics (TCOR and TCOR-Rec) in route selection, TCOR improves packet delivery by up to 9% and 14%, respectively. Additionally, TCOR demonstrates greater resilience to network topology changes and

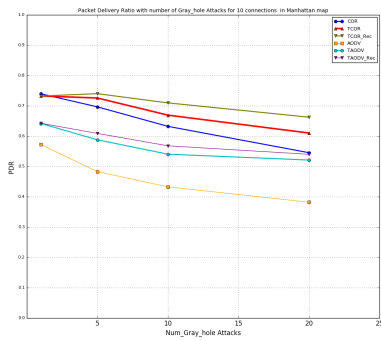


Figure 8: PDR of 10 connections with different number of grey hole attacks in Manhattan map.

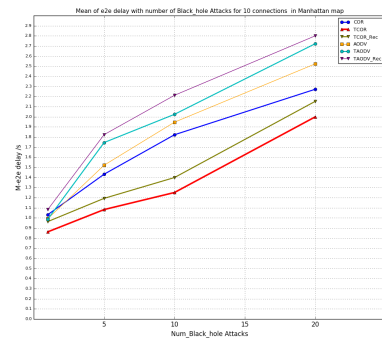


Figure 11: E2e delay of 10 connections with different number of black_hole attacks in Manhattan map.

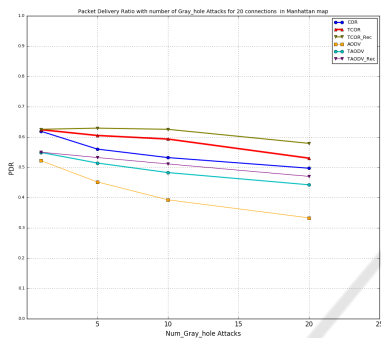


Figure 9: PDR of 20 connections with different number of grey hole attacks in Manhattan map.

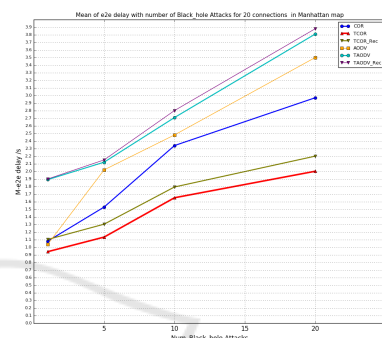


Figure 12: E2e delay of 20 connections with different number of black_hole attacks in Manhattan map.

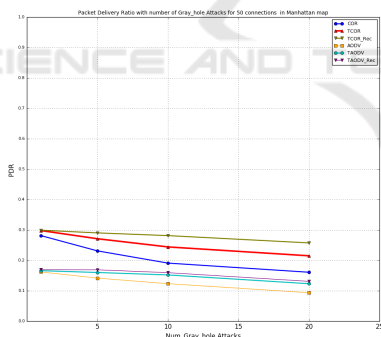


Figure 10: PDR of 50 connections with different number of grey hole attacks in Manhattan map.

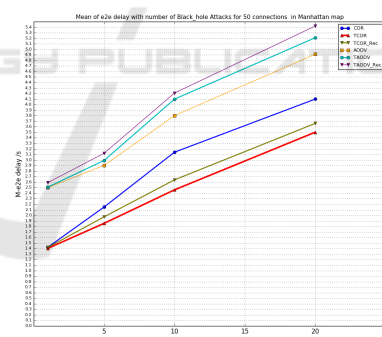


Figure 13: E2e delay of 50 connections with different number of black_hole attacks in Manhattan map.

routing issues, such as packet drops in black-hole or grey-hole scenarios.

Experiments indicate that opportunistic routing protocols outperform traditional AODV and TAODV by approximately 15% in Packet Delivery Ratio and end-to-end delay, even in the absence of network attacks. This highlights their efficiency in reliably delivering data packets in highly dynamic wireless networks.

As future work, VANET routing performance will be further evaluated using additional metrics, such

as jitter, rejected packets, and dropped packets, to achieve optimal QoS for time-critical applications.

In conclusion, the proposed TCOR protocol aligns well with these characteristics and delivers promising results, even in the presence of network issues, including attacks.

REFERENCES

Ben Mussa, S. A., Manaf, M., Ghafoor, K. Z., and Doukha,

- Z. (2016). Simulation tools for vehicular ad hoc networks: A comparison study and future perspectives. *International Conference on Wireless Networks and Mobile Communications, WINCOM 2015*.
- Biswas, S. and Morris, R. (2004). Opportunistic routing in multi-hop wireless networks. *ACM SIGCOMM Computer Communication Review*, 34:69–74.
- Bo, W., Huang, C., Li, L., and Yang, W. (2011). Trust-based minimum cost opportunistic routing for Ad hoc networks. *Journal of Systems and Software*, 84(12):2107–2122.
- Boukerche, A. (2009). Algorithms and Protocols for Wireless Sensor Networks. *Networks*, 6:3722–3725.
- Chandramouli, R., Sinha, M., Dutta, S., et al. (2018). Routing protocols and security issues in manet. In *Proceedings of the IEEE International Conference on Communication Systems and Networks (COMSNETS)*, pages 1–8.
- DLR - Institute of Transportation Systems (2015). SUMO – Simulation of Urban MOBility. *Institute of Transportation Systems*, ””(c):55–60.
- Elakkiya, M., Kaushik, S., and Edna Elizabeth, N. (2014). Opportunistic routing to mitigate attacks in MANET. *2014 International Conference on Recent Trends in Information Technology, ICRTIT 2014*.
- Huangchuanhe, V. (2010). Trust opportunistic routing protocol in multi-hop wireless networks. *2010 IEEE International Conference on Wireless Communications, Networking and Information Security*, pages 563–567.
- Jhanjhi, N., Hossain, M. S., and Yassine, A. (2022). Trust and mobility-based protocol for secure routing in iot networks. *Sensors*, 22(16):6215.
- Kamel, M., Alameri, I., and Onaizah, A. (2017). STAODV: Secure and Trust based Approach to Mitigate Backhole Attack on AODV based MANET. *IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 1:1278–1282.
- Kumar, S. and Banerjee, A. (2017). Cryptographic and trust-based mechanisms in secure routing for manets. *International Journal of Computer Science Issues*, 12(3):45–50.
- Li, N. and Das, S. K. (2013). A trust-based framework for data forwarding in opportunistic networks. *Ad Hoc Networks*, 11(4):1497–1509.
- Luo, H. and Lu, S. (2008). Reputation and Trust-based Systems for Ad Hoc and Sensor Networks. In A. Boukerche, editor, *Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks*, chapter 13, pages 375–405. Wiley.
- Salehi, M. and Boukerche, A. (2014). Trust-aware Opportunistic Routing Protocol for Wireless Networks. *ACM*, pages 79–86.
- Salehi, M. and Boukerche, A. (2015). A Comprehensive Reputation System to Improve the Security of Opportunistic Routing Protocols in Wireless Networks. *2015 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6.
- Salehi, M., Boukerche, A., Darehshoorzadeh, A., and Mameri, A. (2015). Towards a novel trust-based opportunistic routing protocol for wireless networks. *Wireless Networks*, 22(3):927–943.
- Smriti Jain, N. M. J. K. (2017). A survey on trust based secure routing in manet. *RSIS International Journal of Research and Scientific Innovation*, IV(VIII):59–66.
- Thorat, S. A. and Kulkarni, P. J. (2015). Opportunistic Routing in Presence of Selfish Nodes for MANET. *Wireless Personal Communications*, pages 689–708.
- Varga, A. and Hornig, R. (2008). AN OVERVIEW OF THE OMNeT ++ SIMULATION ENVIRONMENT.
- Wang, Z., Member, S., Chen, Y., Li, C., and Member, S. (2012). CORMAN : A Novel Cooperative Opportunistic Routing Scheme in Mobile Ad Hoc Networks. 30(2):289–296.
- Wu, X., Xiao, J., and Shao, J. (2017). Trust-based protocol for securing routing in opportunistic networks. *IEEE International Conference on Automation Science and Engineering*, 2017-Augus:434–439.
- Zhao, Z., Braun, T., Rosário, D., and Cerqueira, E. (2014a). CAOR: Context-Aware adaptive opportunistic routing in mobile ad-hoc networks. *2014 7th IFIP Wireless and Mobile Networking Conference*.
- Zhao, Z., Rosário, D., Braun, T., and Cerqueira, E. (2014b). Context-aware opportunistic routing in mobile ad-hoc networks incorporating node mobility. *IEEE Wireless Communications and Networking Conference, WCNC*, 3:2138–2143.
- Zhizhong, J., Chuanhe, H., Liya, X., Bo, W., Wenzhong, Y., and Xi, C. (2013). Efficient Opportunistic Routing Protocols for VANET. *International Journal of Digital Content Technology and its Applications*, 7(8):11–22.
- Zhizhong, J., Chuanhe, H., Liya, X., Bo, W., Xi, C., and Xiyang, F. (2012). A trusted opportunistic routing algorithm for VANET. *Proceedings of the International Conference on Networking and Distributed Computing, ICNDC*, pages 86–90.