A Novel Indirect Trust Mechanism for Addressing Black hole Attacks in MANET

Hassan Jari
School of Computing, Newcastle
University
Newcastle-upon-Tyne, UK
h.a.m.jari2@ncl.ac.uk

Ali Alzahrani
School of Computing, Newcastle
University
Newcastle-upon-Tyne, UK
a.a.alzahrani2@ncl.ac.uk

Nigel Thomas
School of Computing, Newcastle
University
Newcastle-upon-Tyne, UK
nigel.thomas@ncl.ac.uk

ABSTRACT

Mobile Ad hoc Networks (MANETs) are emerging wireless network with many distinct characteristics. MANET has potential to be useful in different commercial applications. However before doing the same, it is necessary to address various security issues related with MANET. Data routing is one of fundamental operation in the MANET. This research work addresses security issues related with MANET routing protocols. In this paper we consider the performance of MANETs routing protocols subject to a blackhole attack. Trust management aims to protect a network from malicious behaviour. This research work proposed a novel trust-based routing for MANET viz. ITAODV which is derived from regular AODV protocol. The proposed protocol uses indirect trust mechanism which takes into account reliability of each node for forwarding the packets. The performance evaluation of AODV and ITAODV carried out using network simulator NS-3. The experimental results demonstrate effectiveness of the ITAODV protocol against the Black hole attack.

KEYWORDS

MANET, AODV, Black hole Attack, Trust-based routing, Indirect trust, NS-3

ACM Reference Format:

Hassan Jari, Ali Alzahrani, and Nigel Thomas. 2018. A Novel Indirect Trust Mechanism for Addressing Black hole Attacks in MANET. In *Proceedings of ACM Conference (Conference'17)*. ACM, New York, NY, USA, 7 pages. <https://doi.org/10.1145/1122445.1122456>

1 INTRODUCTION AND BACKGROUND

Mobile ad hoc network (MANET) is an emerging technology which does not need fixed infrastructure and centralized administration mechanism for the communication. MANET is also known as wireless ad hoc network. A MANET is generally defined as a mobile network that has numerous autonomous nodes. It is frequently composed of mobile devices or other mobile pieces, which can arrange themselves in various ways and operate without strict rules

of network administration. Due to mobility of nodes MANET topology is dynamic. In MANET nodes broadcast wireless signals for the communication purpose. Due to this each node in a MANET can act as both as a router and as a host. Hence, the nodes need to collaborate for sending data packets from source node to a destination node. In MANET nodes do not belong to single ownership. They are free to join or leave the network at anytime as per their requirements. The MANET nodes may have diverse hardware and software configurations. Generally, the nodes used in MANETs are characterized by less CPU capability, small size memory and are battery operated [7].

A number of routing protocols have been proposed for ad hoc wireless networks. These protocols are based on either distance vector or link state routing algorithms. MANET routing protocols are classified as proactive or reactive depending on whether they keep routes continuously updated or whether they act on demand [6].

Proactive routing protocols are table driven since each node maintains one or more tables containing routing information to every other node in the network. When there is a change in the network topology, updating routing tables must be undertaken throughout the network. This feature is useful for datagram traffic; however, it generates extensive signalling traffic and power consumption [7]. In addition, proactive routing protocols are not suitable for large networks as they need to maintain node entries for every node in the routing table of each node. In table-driven, proactive protocols, the control messages in the network increase due to the message overhead in the network increasing rapidly. There are several well-known proactive routing protocols, such as the wireless routing protocol (WRP), the optimized link state routing (OLSR) protocol and the destination-sequenced distance vector (DSDV) protocol.

Reactive routing protocols are also known as on-demand protocols. In this type of protocol, routes are created whenever a source needs to send data to a destination node, which means that these protocols are initiated by a source on demand [6]. A reactive routing protocol consists of two phases: route discovery and route maintenance. In the first phase, the source code first consults its route cache to check for an available route from the source to destination; if there is no route already available, it will initiate route discovery [2]. In the second phase, route maintenance is undertaken due to the dynamic topology of the network causing an increased incidence of route failure between nodes [2].

One of the advantages of reactive routing protocols is that they can reduce routing overheads because they do not need to search for and maintain routes that do not carry data traffic. However, reactive routing protocols usually take longer routes to send data packets

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

Conference'17, July 2017, Washington, DC, USA

© 2018 Association for Computing Machinery.

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM...\$15.00

<https://doi.org/10.1145/1122445.1122456>

from a source to a destination, causing latency in the network [2]. There are various well-known reactive routing protocols, such as ad-hoc on-demand distance vector (AODV) and dynamic source routing (DSR).

Ad Hoc On-Demand Distance Vector (AODV) is a reactive routing protocol. It enables self-starting, dynamic, and multi-hop routing between participating nodes. It supports nodes to find routes quickly for new destinations because it does not require nodes to maintain inactive routes communication. AODV uses an on-demand approach to discover routes and uses a destination sequence number to discover the most recent path and ensure the freshness of the routes [11]. In addition, it guarantees loop-free routes even while repairing broken routing link [11].

AODV uses a traditional routing table, one entry per destination, and each entry records the next hop to the specified destination and a sequence number generated by the destination to determine whether routing information is up to date and to avoid routing loops. AODV consists of Route Requests (RREQs), Route Replies (RREPs), Route Errors (RERRs) and a HELLO packet for steering in Ad-hoc network [2, 4]. AODV can be used to explore the network topology by broadcasting a HELLO message to the neighbouring mobile nodes. A hello message can detect an invalid link by broadcasting a hello message to mobile nodes in the network.

When a mobile source node needs to communicate with a destination mobile node, it broadcasts an RREQ packet which then creates temporary route table entries for the reverse path on which the RREQ message was transmitted [1]. The mobile source node broadcasts the RREQ to the neighbouring nodes with each node transmitting the RREQ packet to neighbouring nodes until it reaches the destination node. RREQ packets contain a requested destination sequence number, which is one higher than the destination sequence number currently known to the source [1]. The reason for this is to prevent old routing information being used as a reply message to RREQ packets, the main cause of the routing loop issue in a traditional distance vector algorithm [13]. The RREQ counts the number of each node it passes but does not record them. However, each node the RREQ packet passes sets up a temporary reverse link indicating the previous node from which the RREQ packet has come so that the reply can be returned to the source node. When the RREQ reaches the intended destination or an intermediate node that has a fresh route to the destination, it unicasts a reply by sending the RREP packet along with the reverse path established during the route discovery process [1]. The RREP packet contains the total hop count and the destination sequence number of the route. The source node starts sending data packets to the destination node by sending them to each neighbouring node that responds to the RREQ with an RREP until it reaches the destination node. If the transmission breaks in the destination node, the neighbouring nodes will all notice the route breakage due to the movement and subsequently broadcast a route error (RERR) packet to each active upstream neighbour. [12].

The remaining part of this research article is arranged as follows. Section 2 discusses work related to this problem statement. Section 3 discussed basic concepts related with trust management in MANET routing and Blackhole attacks. Section 4 describes the proposed indirect trust mechanism for MANET routing in details.

Experimental observations and analysis is presented in section 5. The conclusions of this research work are given in Section 6.

2 RELATED WORK

Sirisala et al. [10] proposed a WBTQ (Weightage Based Trusted QoS Protocol) that concentrates on both security and quality issue. Encryption algorithms are computationally heavy. Hence rather than using encryption algorithms WBTQ improves network security by calculating each node trustworthiness in participating network operations. WBTQ is an extension to OLSR protocol in which the node trust values and QoS metrics are propagated in the network using the HELLO packets. This protocol provides a flexible and feasible method to the user in choosing a better route by giving weightage to Quality and Trust values [10].

H. Yu et al. [13] defined a trust management system as the degree of assurance for the future behaviour of nodes, based on the previously received services by the nodes. Also, H. Yu et al. classified trust and reputation management system into two major categories which are individual-level trust and system-level trust. Individual-level trust mechanism allows an agent node to collect communication with the subject node, aggregate declarations from other nodes about prospective communication, evaluate the trustworthiness of potential interaction based on the past recorded data, and make a trustworthiness decision on whether to interact with the subject node. System-level trust mechanism concentrates on applying punishment based on the node trustworthiness and reputation to improve the utility achieve for nodes that are highly trustworthy [8].

3 TRUST MANAGEMENT IN MANETS

One of the main vulnerabilities relating to MANETs originate from their open peer-to-peer architecture [9]. MANET routing protocols assume that all nodes collaborate without maliciously disrupting the operation of the protocol and do not provide defence against malicious attackers [6]. Therefore, there is no distinct defence mechanism in MANETs from the security design perspective. In fact, due to the wireless nature of the network in MANETs, the MANET inherits the security threat that is faced by both the wireless and wired networks and even more unique attacks because of its unique characteristics. Additionally, it should be noted that MANET nodes are vulnerable to the Denial of Service (DoS) attack because they have limited computational power as well as limited power capabilities. A further challenge that affects mobile ad-hoc networks greatly is that they experience much higher packets loss because of different factors, for instance increased collisions within the presence of hidden terminals, unidirectional links and repeated path breaks due to the node's mobility [2]. The important goal associated with MANETs is to provide routing security in the network, such as confidentiality, integrity, availability, and anonymity [12]. Trust Mechanism in MANETs can improve with securing the transmission between nodes.

Information sharing and distributed collaboration are essential operations in MANETs to accomplish implementation objective. Collaboration is only a valuable if all participant nodes are operating in trustworthy behaviour. Because MANETs do not have a

centralized control unit to monitor the node operations, a component node has to be cautious when communication with other nodes as the behaviour of nodes can change with the time and environment conditions [4]. Therefore, forming and quantifying behaviour of nodes from a trust perspective is essential for ensuring proper operation in MANETs. In fact, trust in MANETs is mainly important in large scale networks where highly heterogeneous entities participate and high-level nodes collaborations are required. In MANETs, trust management includes trust establishment, trust update, and trust revocation [4]. In addition, it is more challenging to manage trust due to changes in topology caused by node mobility or node failure.

3.1 Black hole attack

A black hole attack is a type of denial-of-service attack that harms the performance of MANET protocols [5]. It has a serious impact on the packet delivery ratio (PDR) and the throughput of the network. The malicious node attracts all packets by falsely claiming to have a fresh, high bandwidth route that is the shortest to the destination node and then drops the packets instead of forwarding them [3]. The black hole attacker continuously observes the network traffic, replies to any route request (RREQ) packets and places itself between the source node and the destination node [3].

Figure 1: Black hole Attack in MANET

Figure. 1 shows how a black hole attack works in the network. Nodes participating in the network are shown by circles. Node A is the source, node B the destination and node C the malicious node. Node A wants to send data to node B. In reactive protocols, such as AODV, a process of routing discovery will initialize to find a fresh and ready route. Node C replies to node A as soon as it receives the RREQ, claiming it has an existing path through it to node B. Node A will just accept the response from node C without any validation and will ignore replies from the other nodes. Node C will start dropping the packets coming from A rather than forwarding them. Such a behaviour by attacking node disturbs entire communication between node A & B.

The research goal of this work is to prevent black hole attack using trust management mechanisms discussed in earlier section.

4 PROPOSED INDIRECT TRUST MECHANISM TO PREVENT BLACK HOLE ATTACK IN MANET ROUTING

A node can calculate trust value using its own observations; such trust is called as direct trust. The direct trust is more useful if the node has sufficient number of observations about every other node participating in the network. However, this is difficult to achieve in a large network wherein there are several nodes who are not in direct contact with each other. Hence it is better to get recommendations from other nodes about the target node. These recommendations after often combined together with own observations to calculate cumulative trust value. This trust value is known as indirect trust.

In the proposed work indirect trust of a node is expressed in terms of reliability and trustworthiness offered by the node in the packet routing process. Each node observes its neighbour for specific events in which are related to the reliability of the packet forwarding ability of the nodes. Each node records positive (α) and negative (β) observations of the neighbour nodes, and then each node calculates the reliability and trustworthiness value of its neighbour node using Bayesian Inference. Bayesian inference is a method of statistical inference in which Bayes' theorem is used to update the probability for a hypothesis as more evidence or information becomes available [12]. The nodes continually exchange their views about the other neighbour nodes' reliability. The node observation parameters are shown in Table 1. Those mechanisms have been implemented into AODV protocol to become the modified AODV with trust based and being called indirect trust AODV (ITAODV).

Table 1 : Observation Parameters Used in ITAODV

Sr.	Observation Parameter – When Recorded	Positive Observation (Alpha)	Negative Observation (Beta)
1	Packet Forwarding Ability – Record for each packet	$\alpha++$ for each packet forward	$\beta++$ for each packet drop
2	Node Battery – Record Value once for new session	$\alpha++$ if Battery Power > 30%	$\beta++$ if Battery Power $\leq$ 30%
3	Node's participation in network routing activities – for each control packet	$\alpha++$ for each control packet initiated by the node	$\beta++$ for RERR control packet destination IP Beta++ if any control packet is dropped
4	Node's packet forwarding queue length – for each new session	$\alpha++$ if Queue empty > 30%	$\beta++$ if Queue empty $\leq$ 30%

A node reliability (r) is the probability that node offers reliable service in packet routing. Node un-reliability (n) is the probability that node packet routing service is un-reliable. Finally, node uncertainty (u) is the probability with which it is not possible to predicate if the node is reliable or not for packet routing.

The above three values together are represented by RNU (Reliability, Unreliability, and Uncertainty). The RNU values can be calculated using direct observations (represented by dt_rnu) and using indirect observations (represented by it_rnu) Each node will do the following:

- Continuously observe α_i and β_i for each neighbour node i
- Using α_i and β_i each node calculates dt_rnu_i of the neighbour node i . Here dt_rnu_i is node reliability, unreliability and

uncertainty which is calculated using direct observations. This calculation is done using Bayesian Inference.

- After periodic interval each node sends dt_rnu_i values to all neighbour nodes t .
- Every node synthesizes received observations and calculate it_rnu_i . Here it_rnu_i is the node reliability, unreliability and uncertainty which is calculated using direct and indirect observations. This calculation is done using weighted average method.

4.1 Calculating Node's RNU using Direct Observations (dt_rnu_i)

The posterior distribution of successful cooperation between two nodes can be represented by a Beta distribution function with density function given in equation 1. The direct node reliability expectation (dt_r) is calculated using equation number 2. The direct node unreliability expectation (dt_n) is calculated using equation number 3. And direct node uncertainty (dt_u) is calculated using equation number 4.

$$Beta(\theta|\alpha, \beta) = \frac{\tau(\alpha + \beta + 2)}{\tau(\alpha + 1)\tau(\beta + 1)} \theta^\alpha (1 - \theta)^\beta \quad (1)$$

Node reliability expectation dt_r is calculated as follows:

$$dt_r = \frac{\alpha}{\alpha + \beta} (1 - u) \quad (2)$$

Node unreliability expectation dt_n is calculated as follows:

$$dt_n = \frac{\beta}{\alpha + \beta} (1 - u) \quad (3)$$

Node uncertainty dt_u is calculated as follows:

$$dt_u = \frac{12\alpha\beta}{(\alpha + \beta)^2(\alpha + \beta + 1)} \quad (4)$$

The dt_rnu_i represents reliability, unreliability, and uncertainty of the node i calculated using direct observations.

4.2 Calculating Node's RNU using Indirect Observations (it_rnu_i)

After periodic interval, each node sends dt_rnu_i values to all neighbour nodes. After receiving these values every node synthesizes received observations and calculate it_rnu_i . Here it_rnu_i is node reliability, unreliability and uncertainty which is calculated using direct and indirect observations. This calculation is done using weighted average method.

The equation number 5 shows calculation of node reliability using indirect method (it_r_i). The equation number 6 shows calculation of node unreliability using indirect method (it_n_i). The equation number 7 shows calculation of node uncertainty using indirect method (it_u_i).

$$it_r_i = \frac{\sum_{0 < i \leq N} r_i * w_i}{W} \quad (5)$$

$$it_n_i = \frac{\sum_{0 < i \leq N} n_i * w_i}{W} \quad (6)$$

$$it_u_i = 1 - (it_r_i + it_n_i) \quad (7)$$

Here, N is number of nodes in the network,

w_i = weight assigned to node i depending on past interactions

W = Cumulative weight

4.3 Modifying AODV Routing Mechanism

The regular AODV routing protocol uses *hop count* as the parameter for taking routing related decisions. This approach is good when all participating nodes are trustworthy and performing their routing related duties as per the expectations. However, when Black hole attack is happening then this approach not useful. To overcome Black hole attack, we modified working of AODV protocol as follows.

In modified AODV viz. ITAODV protocol each node uses synthesized reliability values for making routing decisions. Here, a neighbour node which is nearer to the destination and also reliable is preferred as next packet forwarding node.

Each node finds trust value of every possible packet forwarding node i using equation number 8.

$$Trust_i = \frac{0.4}{\text{No. of Hops to Destination}} + 0.6 * it_r_i \quad (8)$$

In above equation 40% weight is given to hop's nearness to the destination node and 60% weight is given to reliability of the node. The ITAODV protocol uses a neighbour node with maximum trust value to forward a packet from a source node to a destination node.

5 PERFORMANCE EVALUATION AND ANALYSIS

In experimental work, we compared performance of AODV and ITAODV protocols using NS-3 simulator. The performance of protocols measured using 3 different parameters viz. packet delivery ratio (PDR), throughput, and end to end delay. We used 2 different test conditions for performance evaluation purpose viz. different mobility speed and different number of malicious nodes in the network. The details of these test conditions and corresponding observations are given in detail below.

5.1 Performance Evaluation Using Different Mobility Speed

Mobility of nodes is main characteristic of a MANET. Hence it is necessary to evaluate the performance of routing protocols using different mobility speed of the nodes. The simulations are carried out to investigate the effect of nodes mobility speed on both AODV and ITAODV in the presence of black-hole attack. We run the simulation ten times on each different mobility speed to increase the reliability of the simulation results. Table 2 shows network simulation parameters used in this test condition. The simulation was executed for 180 seconds with help a grid having dimension of $800 \times 800 m^2$. We used 15 nodes which are configured to have 1-100 m/s mobility speed and 10 seconds pause time. The UDP traffic having packet size of 512 bytes used during the simulation.

From Figure 2, we can observe that packet delivery ratio in the ITAODV protocol is better than AODV as the mobility speed of nodes increased from 1 to 100 m/s. We can observe that the black-hole attack affected the performance of AODV and ITAODV protocols negatively. The black hole attack causes lot of packet

Table 2 : Simulation Parameters for Different Mobility Speed

Routing Protocols	AODV & ITAODV
Simulation Time	180 sec.
Dimension	800 x 800 m ²
Number of Nodes	15
Packet Size	512 bytes
Mobility model	Random Waypoint
Node Speed	1 - 100 m/s
Pause Time	10 seconds
Traffic Type	UDP

drops. ITAODV protocol is able to reduce these drops by making use of trust in routing decisions.

Figure 2: AODV and ITAODV PDR under Black-hole Attack by Varying Mobility Speed

Figure 3 shows the impact of increasing nodes mobility speed on the performance of AODV, and ITAODV in the presence of black-hole attack in terms of throughput. We can see from the figure that as the mobility speed increases, the throughput of both the AODV and ITAODV protocols predominantly decreases with the effect of the malicious nodes makes the performance even lower. Figure 4 shows the impact of increasing nodes mobility speed on the performance of AODV, and ITAODV in the presence of black-hole attack in terms of delay. The delay in the ITAODV is more as compared to AODV. This is due to ITAODV protocol uses a complex parameter viz. trust for making routing decisions whereas AODV uses hop count as routing decision parameter. ITAODV takes a long time to calculate the trustworthiness value then send the packet using the more reliable route using the indirect trust mechanisms.

5.2 Performance Evaluation by Varying Malicious Nodes

In second test condition we found the experimental results by varying number of malicious nodes in the network. The simulations

Figure 3: AODV and ITAODV Throughput under Black-hole Attack by Varying Mobility Speed **Figure 4: AODV and ITAODV Delay under Black-hole Attack by Varying Mobility Speed**

are done to explore the effect of number of malicious nodes on the network simulator. Figures 5, 6, and 7 show the performance of both AODV and ITAODV under black-hole attack as we increase the malicious nodes.

The simulation parameters used in this test condition are shown in Table 3. The simulation executed for 180 seconds with 80 nodes. The nodes placed in a grid of size of 1000x1000 m². Random waypoint mobility model used with nodes having movement speed of 15 m/s. The test condition uses 5 seconds pause time. The UDP traffic used between nodes during simulation. In this test condition number of malicious nodes varied from 1 to 25. These malicious nodes are performing Black hole attack in the network.

Figure 5 shows the impact of increasing number of malicious nodes on the performance of AODV, and ITAODV in the presence of black-hole attack in terms of packet delivery ratio. From the figure we can observe that packet delivery ratio in the ITAODV protocol is consistently better than AODV as number of malicious nodes increased from 1 to 25. The performance of AODV and ITOADV is almost equal when 1 malicious node is present in the network. However, the difference between performance of these protocols goes on increasing with increase in number of malicious nodes. For 25 malicious nodes PDR of ITAODV is 52% which is significantly

Table 3 : Simulation Parameters for Different Malicious Nodes

Routing Protocols	AODV & ITAODV
Simulation Time	180 sec.
Dimension	1000 x 1000 m ²
Number of Nodes	80
Packet Size	512 bytes
Mobility model	Random Waypoint
Node Speed	15 m/s
Pause Time	5 sec.
Traffic Type	UDP

high as compared to that of AODV. For AODV protocol the PDR is 36% when 25 nodes in the network are malicious.

Figure 5: AODV and ITAODV PDR under Black-hole Attack by Varying Malicious Nodes

Figure 6 shows the impact of increasing number of malicious nodes on the performance of AODV, and ITAODV in the presence of black-hole attack in terms of throughput. From the figure we can observe that throughput in the ITAODV protocol is better than AODV when number of malicious nodes increased from 1 to 25. The throughput of ITAODV protocol decreases from 73% to 33% when number of malicious nodes increased from 1 to 25. The throughput of AODV protocol decreases from 66% to 20% when number of malicious nodes increased from 1 to 25. The AODV protocol is impacted more by presence of malicious nodes in the network.

Figure 7 shows the impact of increasing number of malicious nodes on the performance of AODV, and ITAODV in the presence of black-hole attack in terms of packet end to end delay. From the figure we can observe that end to end delay for AODV protocol is less than ITAODV protocol. The difference between performance of

Figure 6: AODV and ITAODV Throughput under Black-hole Attack by Varying Malicious Nodes

both protocol is almost consistent even though number of malicious nodes in the network are increased.

Figure 7: AODV and ITAODV Delay under Black-hole Attack by Varying Malicious Nodes

6 CONCLUSION AND FUTURE WORK

One of the main vulnerabilities of MANETs lies in their open peer-to-peer architecture. MANET routing protocols assume that all nodes collaborate without maliciously disrupting the operation of the protocol and do not provide a defense against malicious attackers [2]. Therefore, there is no clear line of defense in MANETs from the security design perspective. Indeed, due to the wireless nature of the networks in MANETs, they inherit the security threats faced by both wireless and wired networks and even more attacks because of their unique characteristics. Black hole attacks in MANET routing have potential to disturb communication between the nodes in significant manner.

This research work proposed trust-based approach to overcome Black hole attack in MANET routing. The proposed algorithm uses trust values which are derived using reliability of node for making routing decisions. The reliability values are estimated using past behavior of the nodes in communication process. The proposed

algorithm uses indirect trust model which is more robust for large networks.

We evaluated performance of the proposed ITADOV protocol in comparison with AODV protocol using network simulator using different test conditions. The experimental results show that the ITADOV protocol is stable and performs well under blackhole attack as the nodes mobility speed increase from 1 m/s to 100 m/s in steps of 10 m/s. On the other hand, The AODV protocol performance is impacted negatively as the node mobility speed increases and in the presence of black hole attack, it performs lower than ITADOV in the performance metrics of PDR and throughput while it performs better in the delay metrics. We also observed that as the number of malicious nodes increases the protocols performance decrease as the malicious nodes' behavior are unpredictable. In the case of ITADOV, the malicious nodes do not affect its performance poorly because of the trust base algorithms it uses to send the packets from a source node to a destination node. It is essential to focus on defense when measuring the performance of routing protocols. In addition, AODV has many vulnerabilities so by designing an algorithm to cope with the AODV to enhance its performance to have a secure connection in the network.

In the future, we are planning to expand the simulations to include more protocols, such as temporally ordered routing algorithm (TORA), dynamic source routing (DSR) and optimized link state routing (OLSR) protocols. We are interested to test the behavior of such protocols as we add the trust mechanisms and how they react in different simulations and compare them based on the environment in which the network is to be used.

REFERENCES

- [1] Mohamed A. Abdelshafy and Peter J.B. King. 2013. Analysis of security attacks on AODV routing. *2013 8th International Conference for Internet Technology and Secured Transactions, ICITST 2013* (2013), 290–295. <https://doi.org/10.1109/ICITST.2013.6750209>
- [2] Ali Alzahrani, Hassan Jari, and Nigel Thomas. [n.d.]. Analysing the Effect of Mobility on the Performance of MANET Routing Protocols. ([n. d.]), 1–11.
- [3] Sandeep Dhende, Sandeep Musale, Suresh Shirbahadurkar, and Anand Najan. 2017. SAODV: Black hole and gray hole attack detection protocol in MANETs. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. 2391–2394. <https://doi.org/10.1109/WiSPNET.2017.8300188>
- [4] Raihana Ferdous, Vallipuram Muthukkumarasamy, and Abdul Sattar. 2010. Trust Management Scheme for Mobile Ad-Hoc Networks. In *2010 10th IEEE International Conference on Computer and Information Technology*. 896–901. <https://doi.org/10.1109/CIT.2010.167>
- [5] Danista Khan and Mahzaib Jamil. 2017. Study of detecting and overcoming black hole attacks in MANET: A review. In *2017 International Symposium on Wireless Systems and Networks (ISWSN)*. 1–4. <https://doi.org/10.1109/ISWSN.2017.8250039>
- [6] Marek Natkaniec. 2009. Ad Hoc Mobile Wireless Networks: Principles, Protocols, and Applications (Sarkar, S. K. et al.; 2008) [Book Review]. *IEEE Communications Magazine* 47, 5 (2009), 12–14. <https://doi.org/10.1109/MCOM.2009.4939268>
- [7] Suniti Purbey. 2018. a Review on Manet (Mobile Ad Hoc Network). *International Journal of Emerging Trends in Engineering and Development* 1, 9 (2018), 7–12. <https://doi.org/10.26808/rs.ed.i9v1.02>
- [8] Raghavendar L. Raju and C. R.K. Reddy. 2019. Node activity based trust and reputation estimation approach for secure and QoS routing in MANET. *International Journal of Electrical and Computer Engineering* 9, 6 (2019), 5340–5350. <https://doi.org/10.11591/ijece.v9i6.pp5340-5350>
- [9] Venkata Latha Sai Saranya Kasa, C. Shoba Bindu, and Nageswararao Sirisala. 2018. Trusted Quality of Service Routing Protocol in Mobile Ad-hoc Networks. In *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*. 2269–2273. <https://doi.org/10.1109/RTEICT42901.2018.9012483>
- [10] Nageswararao Sirisala and C.Shoba Bindu. 2014. Weightage based trusted QoS protocol in Mobile Adhoc Networks. In *2014 IEEE Global Conference on Wireless Computing Networking (GCWCN)*. 283–287. <https://doi.org/10.1109/GCWCN.2014.7030895>
- [11] Sandeep A Thorat and P J Kulkarni. 2014. Design issues in trust based routing for MANET. In *Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on*. IEEE, 1–7.
- [12] Meisam Yadollahzadeh-Tabari. 2021. An Stochastic Reward net Model for Performance Analysis of Network layer in Mobile Ad Hoc Network Under the Workload of Misbehavior Nodes. *Wireless Personal Communications* 118, 2 (2021), 1087–1109. <https://doi.org/10.1007/s11277-020-08060-0>
- [13] Han Yu, Zhiqi Shen, Chunyan Miao, Cyril Leung, and Dusit Niyato. 2010. A Survey of Trust and Reputation Management Systems in Wireless Communications. *Proc. IEEE* 98, 10 (2010), 1755–1772. <https://doi.org/10.1109/JPROC.2010.2059690>