Journal of Engineering and Computer Innovations Vol. 2(5), pp. 78-89, May 2011
Available online at http://www.academicjournals.org/JECI
ISSN 2141-6508 ©2011 Academic Journals

Full Length Research Paper

Scenario based performance analysis of reliant ad hoc on-demand distance vector routing (R-AODV) for mobile ad hoc network

H. S. H. Jassim[1]*, S. K. Tiong[1], S. Yussof[2], S. P. Koh[1] and R. Ismail[2]

[1]College of Engineering, Universiti Tenaga Nasional, KM 7, Jalan kajang puchong, 43009 Kajang, Selangor, Malaysia.
[2]College of Information Technology, Universiti Tenaga Nasional, KM 7, Jalan kajang puchong, 43009 Kajang, Selangor, Malaysia.

Accepted date 15, March, 2011

A mobile ad-hoc network (MANET) is a peer-to-peer wireless network, that is, nodes can communicate with each other without the use of infrastructure. Besides, nodes are free to join and/or leave the network at anytime, move randomly and organize themselves arbitrarily. Due to this nature of MANET, there could be some malicious and selfish nodes that try compromise the routing protocol functionality and make MANET vulnerable to security attacks which lead to unreliable routing. The current work presents a reliant ad hoc on-demand distance vector routing (R-AODV) based on trusted and shortest path and compare to AODV trust framework to which have been used to overcome the mentioned problem as well. The performance differentials are analyzed using various metrics which are packet delivery fraction, average end-to-end delay, and normalized routing load. The algorithm is implemented and simulated using NS2. The performance differentials are analyzed using various metrics which are packet delivery fraction, average end-to-end delay, and normalized routing load. The results revealed that the developed R-AODV exhibits good performance. Moreover, the proposed routing mechanism is competitive, as compare to trust ad hoc on-demand distance vector (TAODV).

Key words: Reliability, mobile ad-hoc network (MANET),routing protocol.

INTRODUCTION

Mobile ad-hoc network (MANET) composes only of nodes. These nodes do not have fixed infrastructure or any centralized controller such as access point or server to determine the route of the paths. Thus, each node, in an ad hoc network, has to rely on each other in order to forward packets. Therefore, there is a need to use a specific cooperation mechanism to forward packet from hop to hop before it reaches a required destination by using routing protocol (Perkins and Royer, 2003). Examples of available routing protocols for MANET are ad hoc on-demand distance vector (AODV) (Perkins and Royer, 2003), destination sequenced distance vector (DSDV) (Venugopal et al., 2008), and dynamic source routing (DSR) (Johnson et al., 2007). The main aim of those routing protocols is to find the shortest path in the source-destination routes selection (Buruhanudeen et al., 2007). These routing protocols can be attacked by blackhole (Tamilselvan and Sankaranarayanan, 2007; Seungjin et al., 2004; Irshad and Shoaib, 2010), denial of service DoS (Gupta et al., 2002; Aad et al., 2008), and wormhole (Khalil et al., 2005). These attacks may influence the routing of packets. Therefore, in MANET, misbehaviour nodes, due to selfish or malicious reasons, can significantly degrade the performance of MANET.

Due to security issues that can occur on MANET, researchers have proposed many mechanisms to prevent and reduce the risk. Most of these mechanisms are focused on how to protect the data transmission network such as access control (Miguel et al., 2010), and key

*Corresponding author. E-mail: Hothefa@uniten.edu.my. Tel: +60-176761927.

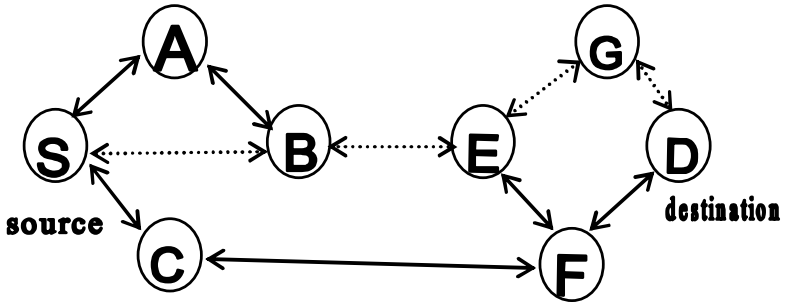

Figure 1. An example of broadcasting RREQ and unicasting RREP between source node S and destination, D.

management (Adams et al., 2005). Meanwhile, there are some works which focused on how to makes MANET routing protocols discover routes in a secure method e. g. trust models mechanisms (Meka et al., 2006; Xiaoqi et al., 2004). Most of the optimizations, in routing protocols, are limited to improving the path resilience and the reliability of packet delivery with secure route. However, current ad-hoc routing protocols have not fully addressed the performance issues related to the security by considering the shortest path.

The current work proposes an implementation of trust mechanism in the ad hoc on-demand distance vector routing protocol (AODV). The new mechanism is called as reliant ad hoc on-demand distance vector routing (R-AODV) that considers both trust and shortest path in making routing decision. Meaning route will be selected based on the trust value assign to each node with the hop count. The performance of R-AODV is compared with AODV trust framework which uses route trust as a metric for the source node to make such informed route selection decisions.

RELATED WORKS

To enhance the performance of routing protocols in MANET, a lot of approaches have been presented so far. The approaches can be mainly classified into two groups: Reliability based approaches (Amir, 2008), efficiency and security based approaches (Tamilselvan and Sankaranarayanan, 2007; Seungjin et al., 2004; Irshad and Shoaib, 2010; Miguel et al., 2010; Adams et al., 2005; Meka et al., 2006). There are quite a number of excellent protocols in terms of efficiency however lacking of the security consideration. Meanwhile, there are good protocols in terms of security too but do not significantly consider network efficiency. In this work, both aspects were considered in designing a new routing protocol. This work present a simple and reliable protocol called a reliant ad hoc on-demand distance vector routing (R-AODV) which simply considering the shortest and the trusted path. The proposed protocol was implemented using network simulation software ver. 2. Similar routing protocol proposed by Meka et al. (2006) has been chosen for comparison in order to evaluate and bench mark the performance of proposed R-AODV protocols under different simulation scenarios.

Review of ad hoc on-demand distance vector routing protocol (AODV)

The most common ad-hoc protocol is the ad hoc on-demand distance vector (AODV) routing protocol (Perkins and Royer, 2003). It is capable of both unicast and multicast routing. It is on demand algorithm, meaning that it builds routes between nodes only when the source node needs it (Gorantala, 2006). Also it is a method of routing messages between mobile computers which allows these mobile computers, or nodes, to pass messages through their neighbours to nodes with which they cannot directly communicate. When one node needs to send a message to another node that is not its neighbour, it broadcasts a route request (RREQ) message. The RREQ message contains: The source, the destination, the lifespan of the message and a sequence number. Once node 1's neighbours receive the RREQ message, there are two options; they will forward the message if they know a route to the destination or they can send a route reply (RREP) message back to the source node if they are the destination. Figure 1 shows an example of broadcasting RREQ and unicasting RREP messages between source and destination nodes. Each node has its own routing table which maintains the following information: Next-hop, sequence number, hop count and information about all other nodes in the network. When a source node wants to send a data packet to some other destinations nodes in the network, it will first check its routing table to see if any valid route to the destination exists. If a valid route exists, the source node will send the packet to the next hop found in the source routing table. In the case where there is no existing valid route in the source routing table, the source node will initiate a route discovery process, by

broadcasting a RREQ message. The RREQ message contains:

1. The source IP address and current sequence number.
2. The destination IP address and destination sequence number (destination sequence number is the last known destination sequence number for this destination).
3. A broadcast ID.

Once intermediate node receives the RREQ message, it will first check if it has an active route, or if the existing destination sequence number value saved in its routing table is smaller than the destination sequence number in RREQ message. If so, it rebroadcasts the RREQ message from its interfaces but using its own IP address in the IP header of the message and the TTL in the IP header will be decreased by one, while the hop count field in the broadcast RREQ-message is incremented by one to account for the new hop through the intermediate node. Nevertheless, if a route already exists in the source IP address and the source sequence number in the RREQ message is greater than the destination sequence number, then the source IP addresses that have been saved in the node's routing table or the sequence numbers are equal, but the hop count as specified by the RREQ message is now smaller than the existing hop count in the routing table. As such, the intermediate node will create or update a reverse route to the Source IP Address in its routing table (Perkins and Royer, 2003).

AODV supports multicast and unicast traffic and it shows only one route to every destination, which constitutes a restrictive characteristic (Johnson et al., 2007). In order to establish routes, routing messages need to be exchanged between the nodes. These messages, routing table and the operations of AODV are described subsequently.

AODV route messages

Route request message (RREQ): A RREQ message is broadcasted by the source node that wants to reach an unknown destination node. A route can be determined when the RREQ message reaches either the destination itself, or an intermediate node that has route to the destination.

Route reply message (RREP): A RREP message is unicasting back to the source node. Since each node receiving the request caches a route back to the source of the request, the RREP message can be unicasted back from the destination node to the source node

Route error (RERR): Nodes monitor the link status of next hops in active routes. When a link break in an active route is detected, a RERR message is used to notify other nodes that the loss of that link has occurred. The RERR message indicates which destinations are now unreachable due to the loss of the link.

Routing table in AODV

In AODV, each node maintains information about other nodes in the network using a routing table. Each routing table entry contains the following information: Destination IP address and destination sequence number, valid destination sequence number flag, network interface, hop count (number of hops needed to each destination), next hop, and lifetime (Expiration time for this route table entry) (Perkins and Royer, 2003).

Reliant on-demand distance vector routing protocol (R-AODV)

AODV can be modified to select a path (called the BestPath (BP)) during the route discovery cycle based on both trust and the number of hops (trusted and shortest path). When the route request and route reply (R-RREQ and R-RREP) messages in R-AODV are generated or forwarded by the nodes in the network, each node appends its own trust to the trust accumulator (trust summation accumulator S(t)) on these route discovery messages. Each node also updates its routing table with all the information contained in the control messages. As the R-RREQ messages are broadcasted, each intermediate node that does not have a route to the destination forwards the R-RREQ packet after appending its trust to the trust accumulator in the packet which is computed by

$$S[t] = \sum_{i=1}^{n} trust_{value}(i) \quad (1)$$

where: *n* is number of hop counts received in one path, *S(t)* is the trust summation accumulator, and $trust_{value}(i)$, trust value of neighbouring nodes in the routing table.

Hence, at any point, the R-RREQ packet contains a list of all the nodes visited with their trust value added to trust summation accumulator *S(t)*.

Whenever a node receives an R-RREQ packet, it will check the updates of the route to the source node. It then checks for the *BestPath*, *(Bp)*, for intermediate nodes which is computed by:

$$BestPath\ (Bp) = \frac{S[t]}{\sqrt{Hop_{count}} \cdot Hop_{count}} \quad (2)$$

where *BestPath (Bp)* is the best path computed based on both trust and hop count from source to destination,

and Hop_{count}, the hop count included in the request message.

If the B*estPath (Bp)* to any of the intermediate nodes is greater than the previously known *BestPath (Bp)* to that node, the routing table entry is updated for that node and a new trust value computed by Equation 3 is assigned.

$$trust_{value\_new} = \frac{S[t]}{Hop_{count}} \quad (3)$$

where $trust_{value\_new}$ is new trust value that will be updated in the routing table.

The concepts of our reliant AODV were presented subsequently.

Route discovery

The goal of this work is for the source node to select a secure route with less hop count to a destination node. The source node, S, broadcasts a route discovery message (R-RREQ) to its neighbours which contains:

S broadcasts R-RREQ:
<Source_Addr, Source_Seq#, Broadcast_ID, Dest_Addr, Dest_Seq#, Hop_Count, S(t), Bp>

Similar to RREQ messages in AODV, when a node receives an R-RREQ message, it sets up a reverse path back to the source by recording the neighbour from which it receives the R-RREQ message. Meanwhile, when the node receives the R-RREQ message, it will check whether it is the destination or not, if so, it will update the routing table for that node and generate an R-RREP message. But if the receiving node is an intermediate node, it attaches the trust value in its routing table to the trust summation accumulator *S(t)* in the message. Upon receiving the message, a node verifies the *BestPath (Bp)* in the routing table with the new *BestPath (Bp)* value attached in the message. If the new *BestPath (Bp)* is bigger than the one in the routing table, the node then updates the routing table.

Route reply

After receiving the R-RREQ message, the destination node creates a route reply message (R-RREP), signs it and unicasts the reply massage back to the source over the reverse path. The destination node, creates the R-RREP message, and sends it back to its neighbour. The route reply message contains:

D unicasts R-RREP:
<Source_Addr, Dest_Addr, Dest_Seq#, Hop_Count, Lifetime, S(t), Bp>

SIMULATION AND RESULTS ANALYSIS

In the simulation, the MAC layer used was the IEEE 802.11 MAC protocol with distributed coordination function (DCF) (Borgia et al., 2003). The MAC layer used Request-to-send (RTS) and clear-to send (CTS) control frames for unicast packet to reduce packet collisions resulting from the hidden node problem. For the radio model, Lucent's WaveLAN (Tuch, 1993; Anastasi, 2003) parameters were used in the simulation. WaveLAN had the transmission range of 250 m and the channel capacity of 2 Mb/s. The simulated nodes were allowed to move randomly according to the random waypoint mobility model (IEEE, 1997). Besides, constant bit rate (CBR) was used as the traffic model and traffic pattern that consisted of maximum 5 CBR sources were initiated randomly by time in the simulation. The parameters that were specified when randomizing the communication pattern were the number of wanted sources, the packet size, the rate of sending and the simulation time. Each of the nodes began transmitting at randomly chosen location inside the simulation area. When the simulation started, the nodes remained stationary during a period of pause time (seconds). The nodes would then select random destination in the simulation area and moved towards that destination.

Three different scenarios were simulated and for each scenario, three performance metrics are measured. For each simulation, there are four test cases:

1. The normal AODV protocol and the network nodes do not drop any packet (AODV-wo-drop).
2. The normal AODV protocol and the network nodes drop data packets based on the trust value given to the node (AODV-w-drop).
3. The proposed R-AODV protocol and the network nodes drop data packets based on the trust value given to the node (R-AODV-w-drop).
4. Related method presented by Meka et al. (2006) called a trust-based framework which uses route trust as a metric for the source node to make such informed route selection decisions.

The performance of the four test cases of routing protocol will be compared. The result of test case (1) represents the behavior of a normal AODV in a perfectly trusted MANET. On the other hand, the result of test case (2) and test case (3) represent the respective behavior of the normal AODV and the proposed R-AODV under the condition that the nodes in MANET may drop packets while the result of test case (4) represents AODV trust framework (AODVTF) under the condition that the nodes in MANET may drop packets.

Table 1. Simulation parameters for scenario 1.

Number of nodes	65 -105 nodes
Simulation time	900 seconds
Map size	500 × 500 m
Max speed	25 m/s
Mobility model	Random way point
Traffic type	Constant bit rate (CBR)
Packet size	512 bytes
Connection rate (Nominal radio range)	4 pkts/s
Pause time	0 s
Number of connection	5

Theoretically, it is expected that the proposed R-AODV routing protocol will achieve higher packet delivery rate compared to the normal AODV in the situation where the nodes can drop packets. Of course, the highest packet delivery rate is achieved when the nodes do not drop packets at all (test case (1)). When it comes to end-to-end delay, it is expected that R-AODV protocol will have slightly higher delay compared to AODV due to the possibility that it may take a longer path which is more trusted. The normalized routing load for R-AODV also is expected to be slightly higher compared to that of AODV due to the fact that it will generate more messages if a longer path is chosen.

Scenario 1 performance and analysis

In the simulation of scenario 1, nodes are free to move arbitrarily; thus, the network topology which is typically multihop may change randomly and rapidly at unpredictable times. In this simulation, the number of nodes was varied and they were equally distributed within 500 × 500 m area and the transmission range is 250 m while the simulation period is 900 s. Nodes are increased by 10 for each new simulation until the number of nodes reaches 105. The maximum speed was fixed to 25 m/s and the pause time was 0 s for every simulation. The simulation parameters for this scenario are shown in Table 1.

After each route discovery, nodes will update their routing table based on the highest trust value with less hop count replied. Hence the operation of sending packets will be distributed according to the best path selected in the routing table. Thus, the packet drop rate due to nodes misbehaviours will be reduced. Figure 2 illustrates that AODV has higher packet delivery without drop effect while R-AODV obtained about 10% higher than AODV with drop which obtained about 60% of packet delivery. R-AODV is much better than AODV with drop and AODVTF except when the number of node is small. R-AODV seems very close to AODV with drop in small number of node. The reason is that there is small number of nodes travel in big simulation area, 500 × 500 m. R-AODV seems very close to AODVTF in term of packet delivery fraction in this scenario because they are depending on the trusted path. R-AODV shows much better performance in terms of packet delivery fraction in scenario 1.

Packet delivery fraction of the four test cases is shown in Figure 2. In scenario 1, AODV without drop performed particularly well, while the packet delivery fraction of R-AODV is better than that of AODV with drop regardless of the degree of mobility. The reason is that R-AODV node selects a new and trusted route in the route discovery procedure by using the best path mechanism to transmit data packets to destination. The use of trusted route reduces the possibility of route breakdown caused by packet drop. Therefore, R-ADOV was dropping less number of packets compared to AODV with drop and AODVM with drop while Figure 3 shows the average end-to-end delays for scenario 1 of all the four test cases. The results for the four test cases are almost similar except in AODVTF with drop which has longer delay compared to another three case. In R-AODV, high average end-to-end delay is caused by the selection of best path mechanism. Another reason is that R-AODV has trust value and best path value in the routing control message. These values was computed subsequently during the routing discovery process according to selection path mechanism proposed in (section 3), which cause a slightly longer delay. Theoretically, the expected result for R-AODV should be very high in terms of average end-to-end delay. However, the experiment result of R-AODV showed good performance in term of average end-to-end that might be due to the best path mechanism in R-AODV which is also based on less hops count.

Figure 4 illustrates the normalized routing load of all the four test cases. In this scenario, AODV without drop effects performed particularly well. The result for the four test cases show that R-AODV has higher percentage of normalized routing load because R-AODV depends on the trusted path which may have more hops count compared to the original AODV without drop and AODV with drop which depend on the shortest path only. As a

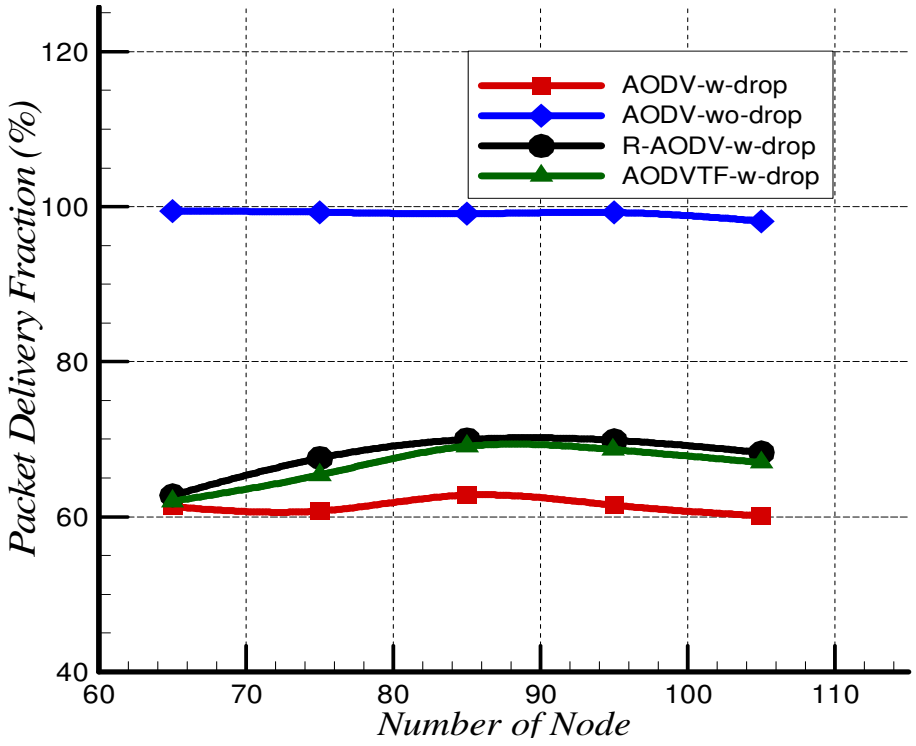

Figure 2. Packet delivery fraction for scenario 1.

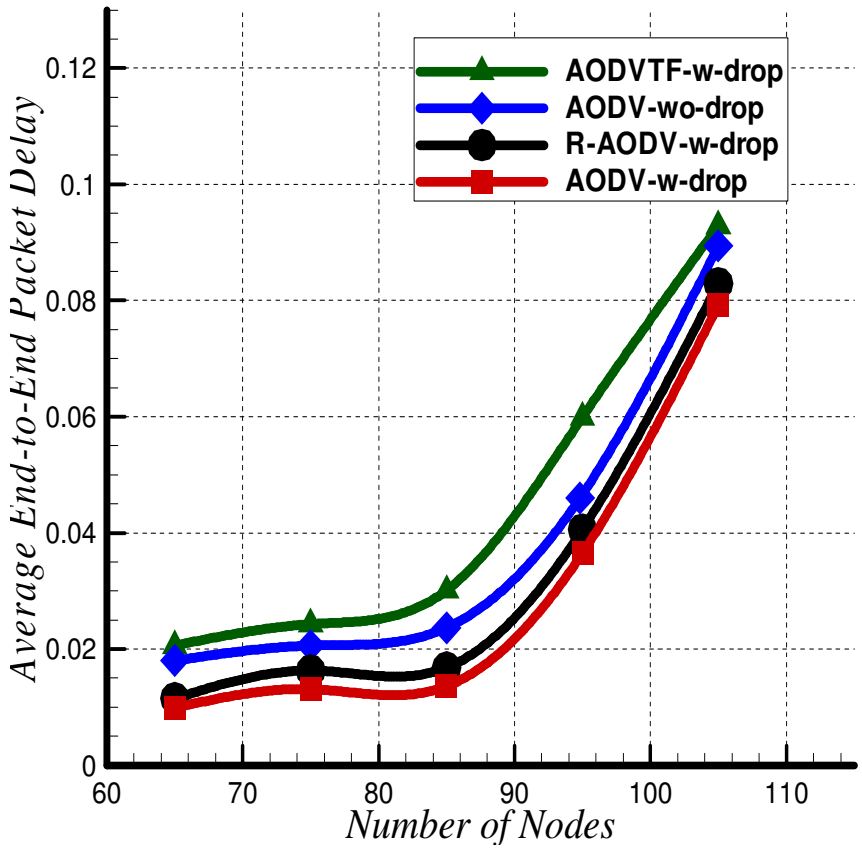

Figure 3. Average end-to-end delays for scenario 1.

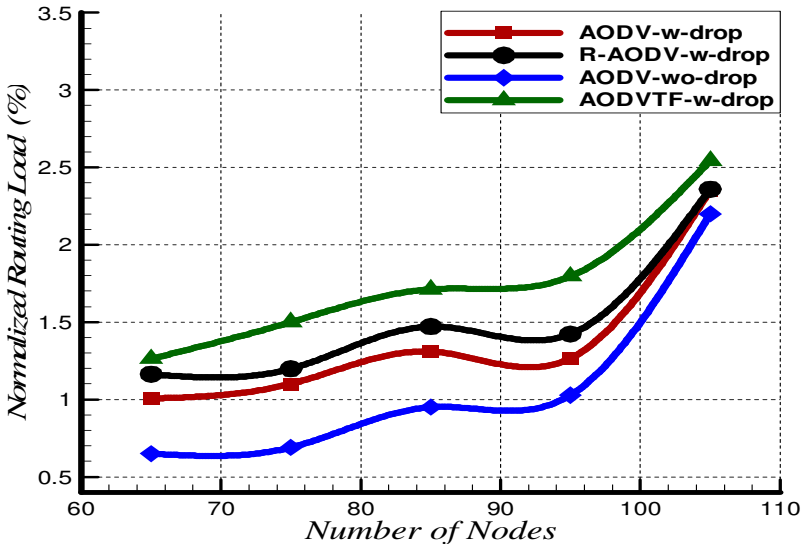

Figure 4. Normalized routing load for scenario 1.

Table 2. Simulation parameters for scenario 2.

Number of node	50 node
Simulation time	900 s
Map size	500 × 500 m
Max speed	25 m/s
Mobility model	Random way point
Traffic type	Constant bit rate (CBR)
Packet size	512 bytes
Connection rate (Nominal radio range)	4 pkts/s
Pause time	0, 25, 50, 75, 100, 125 (s)
Number of connection	5

result, R-AODV will generate more TRREQ and TRREP messages. Theoretically, the expected result for R-AODV should be very high in terms of normalized routing load compare with the other two test cases due to the selection of best path mechanism which depends on the trusted path. However, the experiment result of R-AODV in terms of normalized routing shows that R-AODV performed well with a slightly higher normalized routing load compared to AODV with drop effects.

Scenario 2 performance and analysis

In scenario 2, 50 nodes are fairly distributed within 500 × 500 m area with transmission range is 250 m. Besides, the pause time is varying from 0 to 125 and the simulation period is 900 s. Nodes are allowed to go up 25 m/s which are a reasonably maximum speed. The simulation parameters for this scenario are shown in Table 2.

Figure 5 illustrates the packet delivery fraction of all the four test cases. In this scenario, when pause time is set to 20 which is close to 0 (continuous motion), each of them obtained lower packet delivery fraction. The reason is changing of the topology of network, caused by high motion of nodes due to less pause time. As the pause time reaches 100 (no motion), packet delivery fraction for R-AODV with drop is increased due to the stable network. In summary, for node equal to 50, high values of pause time and simulation area 500 × 500 m, R-AODV with drop effects shows much better performance in the terms of packet delivery fraction compared to AODV with drop.

Figure 6 shows the average end-to-end delay for scenario 2 for all the four test cases. The break in routes in the four test cases lead to nodes discovering new routes which lead to longer end-to-end delay while the source packets are buffered at the source during route discovery. Simulation area plays a role in affecting the performance of the four test cases due to the far distance

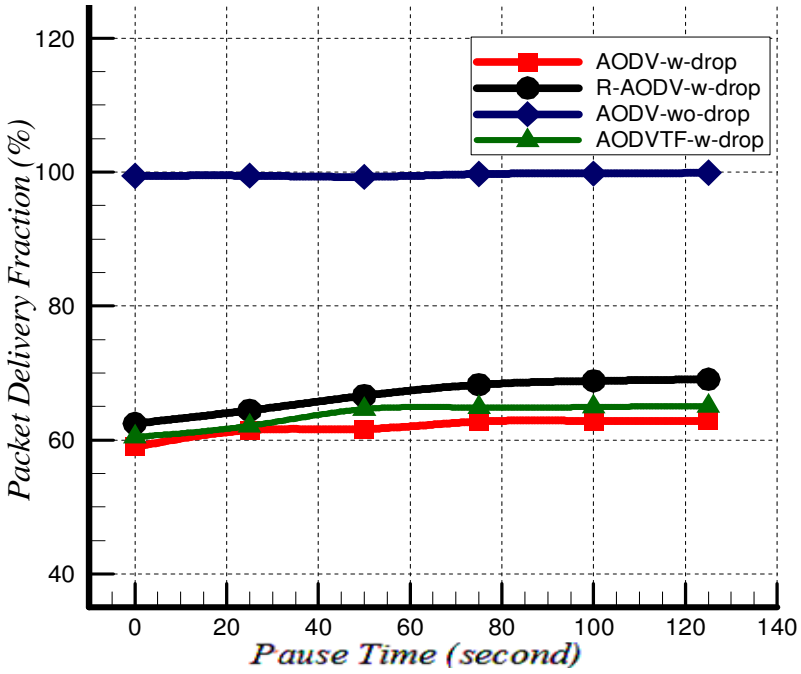

Figure 5. Packet delivery fraction for scenario 2.

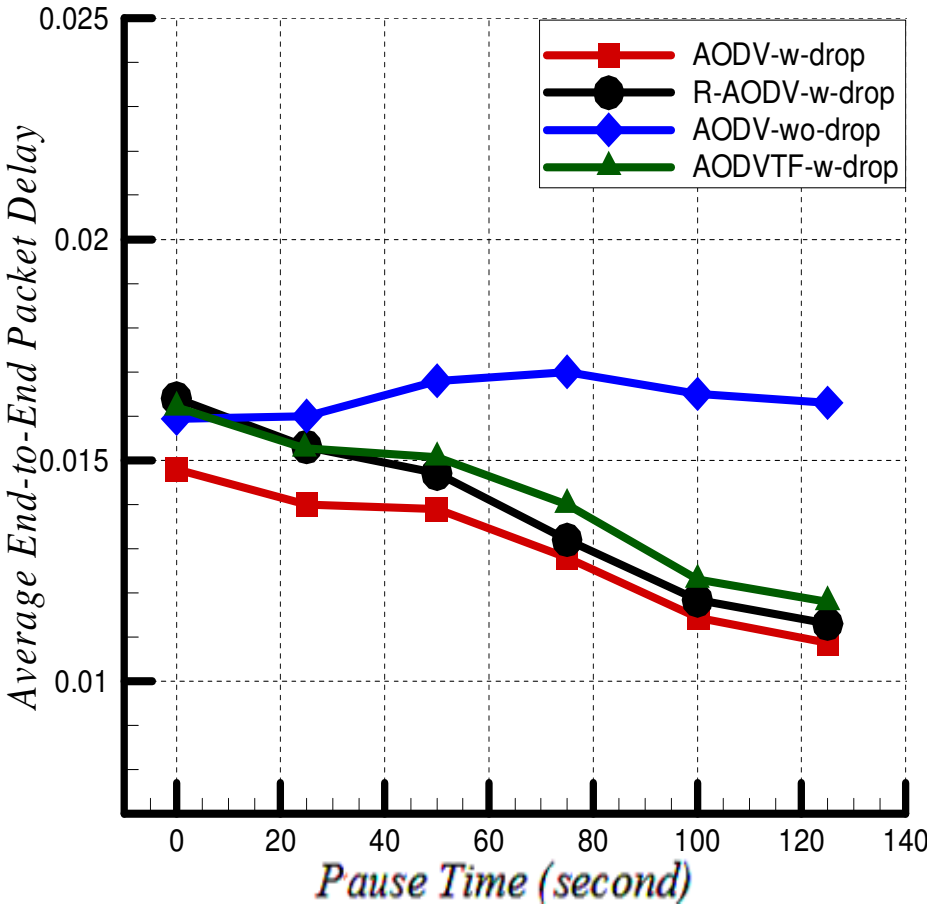

Figure 6. Average end-to-end delay for scenario 2.

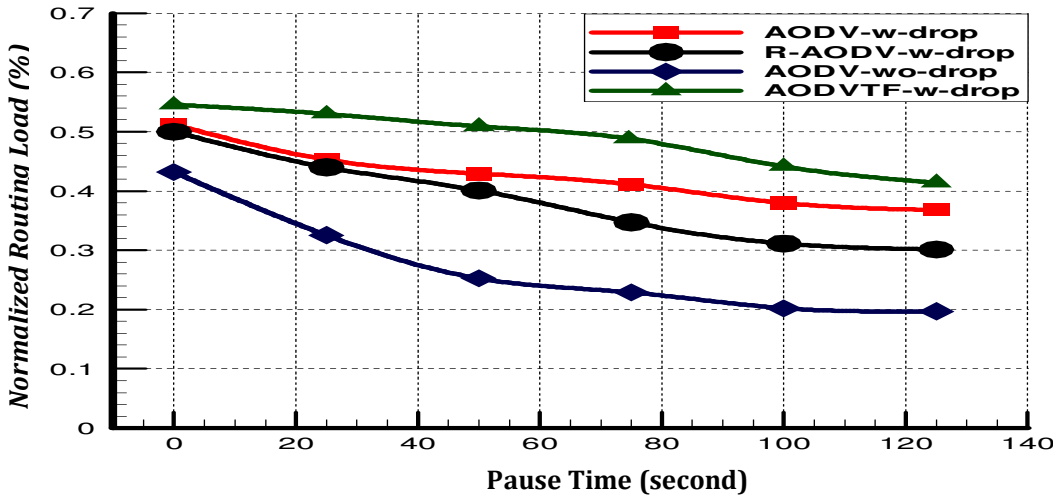

Figure 7. Normalized routing load for scenario 2.

between nodes. In this case, the packet may take longer time in buffering till the next motion. Therefore, all the four test cases may have higher average end-to-end delay. In theory, R-AODV with drop should have very high average end-to-end delay compared to the other two test cases due to the trusted path that has been selected by best path mechanism. This experiment showed that R-AODV with drop has a slightly higher average end-to-end delay compared to AODV with drop. The gap between R-AODV with drop and AODV with drop in end-to-end was reduced when the values of the pause time were increased. R-AODV with drop in scenario 2 shows good performance in term of average end-to-end delay.

Figure 7 illustrates the comparison between the four test cases in terms of normalized routing load. In R-AODV, source node may select the trusted path to destination node which may have much of hop count compared to normal AODV which select the shortest path only. As a result, R-AODV may have much TRREQ and TRREP messages. Sources nodes may have routes break to destination. In this case, nodes need to send RRER message to notify other nodes about that routes break. Hence, nodes have to discover new routes by sending other RREQ messages. Once these RREQ messages received, destinations will generate RREP message. Theoretically, R-AODV should have very high normalized routing load caused by these messages. However, R-AODV with drop in this simulation experiment if this scenario showed better performance in term of normalized routing load compared to AODV with drop.

In this scenario, at pause time equal to 0 (continuous motion), each of the four test cases shows high routing normalized load due to routes break or change in route directory caused by the high motion of nodes. Hence, when the pause time increased to reach no motion, normalized routing load was lower due to the stability of nodes motion. In summary, for fix number of nodes equal to 50 and small spaces, for example 500 × 500 m, R-AODV perform very well and show excellent performance in terms of normalized routing load.

Scenario 3 performance and analysis

In this scenario, 50 nodes are equally distributed in 500 × 500 m area with 250 m as transmission range. Nodes are free to move arbitrarily; thus, the network topology which is typically multihop may change randomly and rapidly at unpredictable times. In this scenario, the mobile nodes move with a speed which varied between 25 to 105 m/s while the pause time was 20 s. The simulation parameters for this scenario are shown in Table 3.

Figure 8 shows the comparison between the four test cases in term of packet delivery fraction. In this scenario, as the maximum speed of node is low, the packet delivery fraction will be higher because the nodes in the network border move slowly toward the network center and the load density of the network center does not change very much. Therefore, the four test cases performed much better when the maximum speed is low, AODV without drop performed particularly well while AODV with drop packet obtained very low percentage of packet delivery fraction. R-AODV with drop obtained almost 70% of packet delivery fraction which is higher than AODV with drop by almost 10%. R-AODV with drop shows much better performance in the terms of packet delivery fraction compared to AODV with drop.

Theoretically, pause time equal to 20 s (almost continuous motion) with varied movement speed will generate unstable network. Therefore, the expected result for R-AODV should be very high in term of average end-to-end delay. The experimental results in this scenario showed that R-AODV has a slight delay due to

Table 3. Simulation parameters for scenario 3.

Number of nodes	50 nodes
Simulation time	900 s
Map size	500 × 500 m
Maximum speed	25-105 m/s
Mobility model	Random way point
Traffic type	Constant bit rate (CBR)
Packet size	512 bytes
Connection rate (Nominal radio range)	4 pkts/s
Pause time	20 s
Number of connection	5

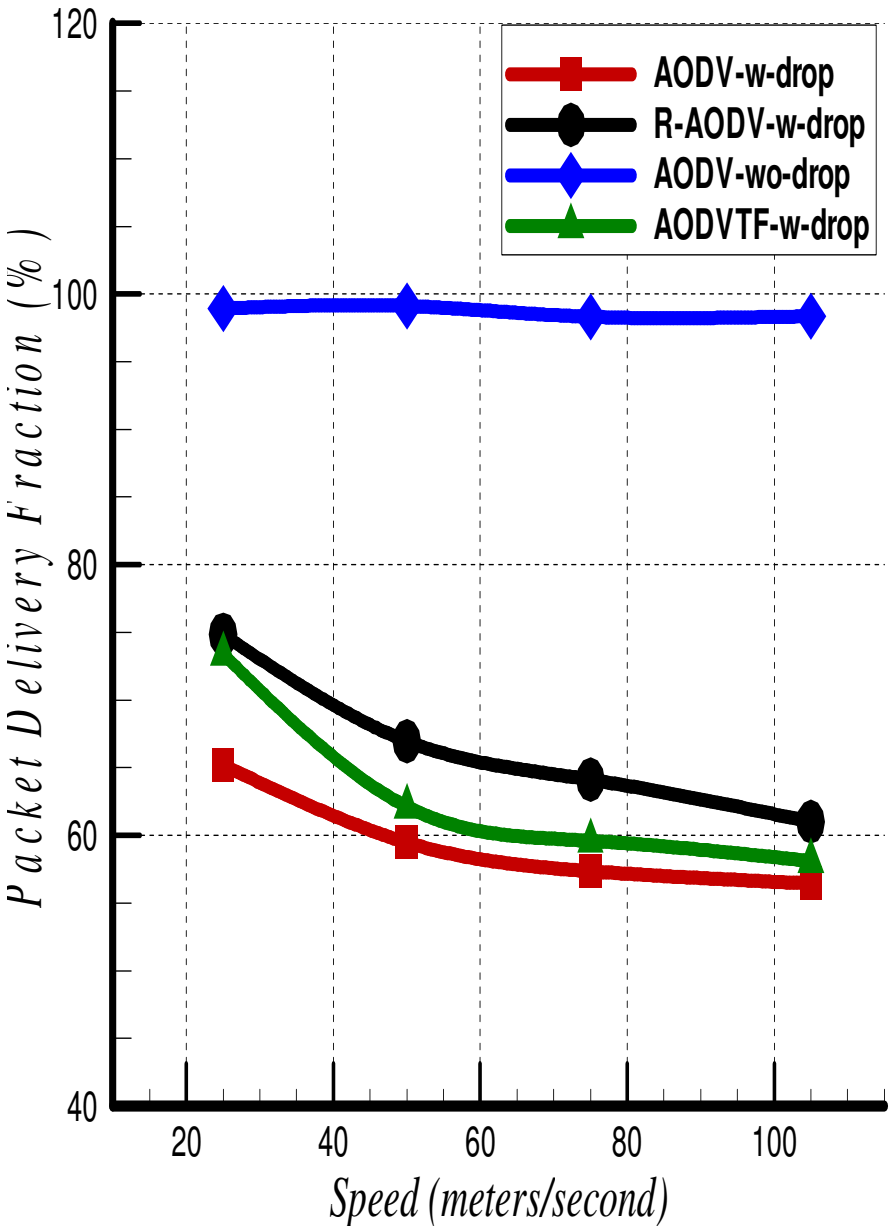

Figure 8. Packet delivery fraction for scenario 3.

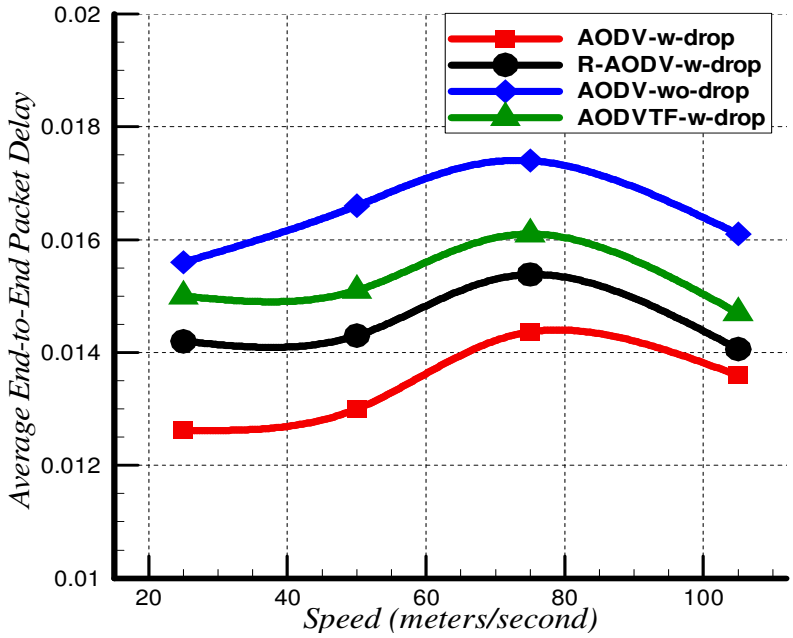

Figure 9. Average end-to-end delay for scenario 3.

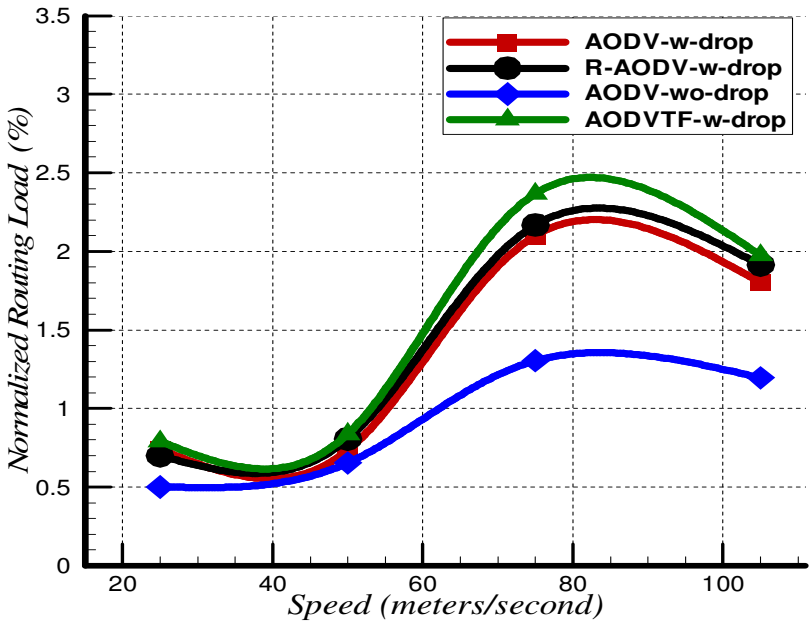

Figure 10. Normalized routing load for scenario 3.

unstable network as shown in Figure 9. On the other hand, R-AODV shows good performance in term of average end-to-end delay.

Theoretically, the source node in AODV without drop and AODV with drop need few RREQ and RREP messages to discover the new route to destination because the routing discovery in these two test cases is based on the shortest path while source node in R-AODV may need much of TRREQ and TRREP messages to discover the new route to the destination. As a result, the expected result for R-AODV with drop should be very high in term of normalized routing load. This experiment showed that R-AODV with drop has a slightly higher normalized routing load compared to AODV with drop as shown in Figure 10. Therefore, R-AODV showed good performance in terms of normalized routing load.

CONCLUSION AND FUTURE WORKS

In this paper, we proposed a new MANET routing algorithm called reliant-AODV (R-AODV) which is basically an extension to the AODV routing protocol that incorporates a trust mechanism to enhance its reliability. The proposed algorithm was implemented and simulated using the NS-2 network simulator. In the simulation used, each node is given a trust value and this value is associated with the possibility of the node to perform a packet drop. With the inclusion of trust mechanism, it is expected that using R-AODV would result in a higher percentage of successful data delivery as compared to AODV. However, it is also expected that due to the extra processing done and the possibility that the packets may take a longer route. Besides, the normalized routing load and end-to-end delay are anticipated to be increase too. Based on the simulation result, the use of R-AODV does provide a higher percentage of successful data delivery. Meanwhile, the simulation has also shown that the impact to normalized routing load and end-to-end delay is very minimal. Therefore, it can be concluded that R-AODV does provide enhanced reliability with minimal impact to performance.

In the future works, research will be carried out to optimize the reliant-AODV routing algorithm and establish some fast response mechanisms when malicious behaviours of attackers are detected. Then, the trust model will be farther applied into other application such as key management. A detailed simulation evaluation will be conducted in terms of packet delivery fraction, message overhead, and security analysis.

REFERENCES

Aad, Hubaux J, Knightly WE (2008). Impact of Denial of Service Attacks on Ad Hoc Networks. Networking. IEEE/ACM Trans., pp. 791- 802.

Adams W, Davis N, Hadjichristofi (2005). A Framework for Key Management in a Mobile Ad-Hoc Network. Proceedings of the International Conference on Information Technology Coding and Computing (ITCC 05), pp. 568-573

Amir Pirzada A (2008). Reliable Routing in Ad Hoc Networks Using Direct Trust Mechanisms. School of Computer Science and Software Engineering. The University of Western Australia. Crawley, 6: 131-157.

Anastasi G, Borgia E, Conti M (2003). IEEE 802.11 ad hoc networks: performance measurements. Icdcsw., 23rd International Conference on Distributed Computing Systems Workshops (ICDCSW'03), p. 758.

Borgia E, Anastasi G, Conti M (2003). IEEE 802.11 ad hoc networks: protocols performance and open issues. Ad hoc Networking. IEEE Press Wiley. New York, pp. 21-26.

Buruhanudeen S, Othman M, Ali BM (2007). Existing MANET Routing Protocols and Metrics used Towards the Efficiency and Reliability-An Overview. Telecommunications and Malaysia International Conference on Communications, IEEE Int. Confer., pp. 231-236.

Gorantala (2006). Routing Protocols in Mobile Ad-hoc Networks. Master's Thesis in Computing Science, Ume°a University. Department of Computing Science, Sweden, pp. 32-48.

Gupta V, Krishnamurthy SV, Faloutsos M (2002). Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks. In Proc. of MILCOM, pp. 202-215.

IEEE (1997). Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) Specifications. IEEE Std., 802: 11.

Irshad U, Shoaib R (2010). Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols. Master thesis report to COM/School of Computing, Blekinge Institute of Technology, Sweden: MEE, 10: 62.

Johnson D, Hu Y, Maltz D (2007). The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, p. 4728.

Khalil I, Bagchi S, Shroff N (2005). LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks. In the International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan, pp. 612-621.

Meka K, Virendra M, Upadhyaya S (2006). Trust based routing decisions in mobile ad-hoc networks. In Proceedings of the Workshop on Secure Knowledge Management (SKM), pp. 41-56.

Miguel P, Ruiz M, Marin RL (2010). Enhanced access control in hybrid MANETs through utility-based pre-authentication control. J. Wireless Comm. and Mobile Comput., pp: 90-96.

Perkins CE, Royer EM (2003). Ad hoc On-Demand Distance Vector (AODV) Routing. IEFT Network Working Group, p. 3561.

Seungjin P, Al-Shurman M, Seong-Moo Y (2004) Black Hole Attack in Mobile Ad hoc Network. ACMSE'04. Huntsville. AL. USA pp: 50-56.

Tamilselvan L, Sankaranarayanan V (2007). Prevention of Blackhole Attack in MANET. Wireless Broadband and Ultra Wideband Communications. AusWireless, pp. 21-21.

Tuch B (1993). Development of WaveLAN, an ISM Band Wireless LAN. AT and T Tech., pp. 27-33.

Venugopal A, Khaleel K, Rahman Ur, Zaman (2008). Performance Comparison of On-Demand and Table Driven Ad Hoc Routing Protocols Using NCTUns. Computer Modeling and Simulation. UKSIM. Tenth Int. Confer., pp. 336-341.

Xiaoqi Li, Michael R. Lyu, Jiangchuan Liu (2004). Trust Model Based Self-Organized Routing Protocol for Ad Hoc Networks. IEEE Aerospace Conference, Big Sky, MT, pp. 2806-2821.