Trusted Route of Spatial Disjoint Multipath Routing Over MANET

Musab Ahmad AL-Tarawni
Dr. Mohd.Yusoff Jamaluddin

Department of Electrical Electronic and System Engineering
Faculty of Engineering and Built Environment
National University of Malaysia (UKM)
43600, Bangi, Selangor
Malaysia.

Abstract

Mobile Ad-hoc Networks (MANET) are acknowledged to be a strong technology, which have attracted many research endeavours in recent years. Although, the theory of wireless, structure-less, dynamic networks is attractive, there are still several major imperfections that avoid industrial growth. Security is just one of these primary obstacles; MANET are known to be specifically subject to the risk of a security strike. One solution offered is to improve the security strength by using multipath routing algorithms. However, multipath routing also presents new issues when it comes to security and security overheads. In this paper, we look at the difficulty of protected routing and expose the TRSDMP protocol. The outcomes reveal that TRSDMP as compared with (AOMDV), raises the network throughput and minimizes the quantity of each discovery overhead, end-to-end delay, also improve the security of the multipath routing

Keywords: MANET; Multipath Routing; Spatial Disjoint Multipath Routing; TRSDMP.

1.Introduction

Wireless networks have received considerable attention in recent years, due to their increased usage and application in mobile phones, laptops or personal digital assistants (PDAs), etc. Infrastructure-less wireless networks or MANET (Mobile Ad Hoc Networks), are a type of Wireless network category that does not consist of a Base Station (BS) to connect a wired Local Area Network (LAN), and, consequently, in MANET, each node has the responsibility to manage the routes in its range.

Routing is a fundamental issue of networks. One of these challenges that create the propose of mobile ad hoc network routing protocols a complicated task. The lack of infrastructure in the wireless network makes it vulnerable to many types of attack (Mavropodi and Douligeris, 2006), and it is very difficult to secure due to the fact that transmission medium is open to anyone within the geographical range of a transmitter.

There are specific types of attack that can appear in MANETs, such as denial of service attacks that cause the total interruption of the routing task, and, therefore, the total process of the ad hoc network (Argyroudis and O'Mahony, 2004), and lack of cooperation attacks that happen when the node does not provide its services to other nodes to save its own resources, such as computation power and energy (Berton et al., 2006).

While encryption of wireless traffic can be achieved, it is usually at the expense of increased cost and decreased performance. Many routing protocols have been proposed to solve the security problems that emerged in MANET. The rest of the paper is structured as follows. In section 2 we review related work. Section 3 explains the TRSDMP protocol. Section 4 shows and analyses protocol performance based on GloMoSim simulation. Finally, in Section 5 we summarize our conclusions and discuss possible future work.

2. Literature Review

Many researchers have focused on multipath routing protocols. Multipath on-demand routing protocols try to identify multiple paths at both the traffic sources and at intermediate nodes in the attempt to find a single route, and provide a secure path for multipath routing protocols. In this section, we will provide a related work of the Multipath Routing in MANET, and Secure Routing Protocols for MANET.

2.1. Multipath Routing in MANET

Multipath routing protocols try to identify multiple paths at both the traffic sources and at the intermediate nodes in the attempt to find a multiple routes. Multipath routing also provides a higher bandwidth and effective load balancing since the load of data forwarding can be distributed over the existing paths (Meghanathan, 2007). In addition, the multiple paths are utilized as a backup or auxiliary method in most multipath routing protocols.
The Ad Hoc On-demand Distance Vector Routing (AODV) protocol is a reactive routing protocol that maintains information when only routes are needed, and builds a single loop free path to each other node in the network, only one path is saved although extra packets are sufficient to construct more than one path. On the other hand, Ad hoc On-demand Multipath Distance Vector Routing (AOMDV) is a multipath extension of AODV that computes multiple loop free link-disjoint routes. Each node has a routing table that keeps routing information for the destination. Periodic hello messages are used to detect and monitor links to neighbours and to update the routing table (Marina and Das, 2001).

When a traffic source needs a route to a destination in AOMDV, it starts the route discovery process. A route discovery process is initiated by flooding the Route Request (RREQ) packet across the network and waiting for a Route Reply (RREP) message. Any intermediate node receiving a RREQ sets up a reverse path to the source, and, if it has a valid route to the destination, it will generate a RREP, otherwise it will rebroadcast the RREQ packet. As the destination node receives a RREQ, it also generates a RREP. The generated RREP will be sent directly to the source using the reverse path. The ad-hoc On-Demand Multipath Distance Vector routing protocol (AOMDV) is modified to discover a set of node-disjoint paths, which are spatially separated. This features used in our propsed protocol based on AOMDV. The route discovery process is initiated by flooding a RREQ packet across the network and waiting for a RREP. Through this The list of paths included in the RREQ message helps in deciding whether a specific route satisfies the disjointness property or not.

2.2. Secure Routing Protocols for MANET

Since security is an essential issue in ad hoc networks, many secure routing protocols have been proposed to address the security challenges and issues related to routing in ad hoc networks.In (Han et al. 2006), Multipath Security Aware Routing (MP-SAR) is suggested as an improvement of the existing Security Aware Routing (SAR) protocol. MP-SAR keeps data confidentially offered by SAR and increases the performance of the data transmission speed.

The existence of multiple paths between nodes in an ad hoc network provides a solution for securing data transmission. The new solution, which focuses on data security transmitting aspects, is called Secured Data based Multipath routing protocol (SDMP). This protocol uses the advantage of the fact that even if an attacker succeeds in having one or lots of transmitted parts, the probability of the original message reconstruction is low (Bouam and Benothman, 2003). In (Talipov et al. 2006), the authors propose a path hopping method based on R-AODV (Kim et al, 2006). Path Hopping Reverse AODV (PHR-AODV) provides an analytic method to determine the intrusion rate. In addition, the authors present a path hopping routing mechanism to build a complete or partial node-disjoint multipath depending on the network topology. Secure Ad hoc On-demand Distance Vector (SAODV) is an offer for a security extension to the AODV protocol (Zapata and Asokan, 2002). In SAODV, every route discovery that is initiated by a node corresponds to a new one-way hash chain.

3. Trusted Route Of Spatial Disjoint Multipath Protocol (TRSDMP)

TRSDMP this protocol chooses the most spatially disjointed paths, which could join partially via nodes that specify a certain security threshold. Using TRSDMP, choosing parted disjoint paths that are more secure, could be better than choosing other maximally spatially disjoint paths that are less secure. TRSDMP inserts in the RREQ message the trust level of the node participating in the route path, and the route list in the AOMDV RREQ message. Figure 1 shows the new RREQ message used in TRSDMP. The Trust-Level List carries the trust value of each node participating in the Route-List.

Type	Flags	Hop Count
Last Address		
Next to Last Address		
Broadcast ID		
Destination Address		
Destination Sequence Number		
Originator Address		
Originator Sequence Number		
Route List		
Trust Level List		

Figure 1. TRSDMP RREQ Message Format.

In TRSDMP, the maximally node disjoint characteristic is adjusted to make the path become partially disjointed via nodes that specify a certain trust threshold. When an intermediate node checks the disjointness of a certain path and there is a common node in this path, a check of the trust level of this common node is made. If the trust level of the common node exceeds a certain threshold value, this path will be considered in the selection process of a multipath. Through TRSDMP, the trust value must be added to the Trust-Level List in the RREQ packet. Any node checks the disjointness of the path and before generating a RREP packet on a specific path it must check the Trust level of all the nodes participating in the path. If the path has a node with a trust value less than a certain trust threshold this path will not be used and the RREQ will be discarded.

3.1. Performance Metrics

In this paper, the Global Mobile Information System Simulation Library network simulator (GloMoSim) was used to evaluate the performance of the TRSDMP that compared with AOMDV. In the experiments, we have conducted in this paper the simulation modelled a network of 100 mobile hosts located at random in a 2000X2000 metre area. We used Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. In the scenarios of experimentation, the mobile nodes have been moving randomly for a simulation time of 400 seconds. Each node moves independently according to the random waypoint mobility model with a 25 (Metre/Second) as maximum mobility speed and 25 sec as pause time.

We use the following performance metrics to compare the performance of the TRSDMP and AOMDV protocols: Network Throughput, Average end-to-end Delay, Packet delivered successfully from the sources to the destinations, and Routing Overhead.To show the enhancement obtained by TRSDMP regarding the selected performance metrics and parameters that present the improvement ratio to help in the comparison between TRSDMP and AOMDV. The Enhancement Ratio (ER) of both protocols can be computed according to Formula 1.

$$ER = (T - A) / T \quad (1)$$

Where T: value of TRSDMP

A: value of AOMDV.

4. Results and Discussion

In this section, we present the results and their analysis of the TRSDMP protocol regarding the mentioned performance parameters and metrics. We compare the results of the proposed TRSDMP with AOMDV.

4.1. Traffic Load

Increasing the number of packets the traffic source has to send, ranging from 20, 40, 60, 80 to 100 packets to change the traffic load of the network.

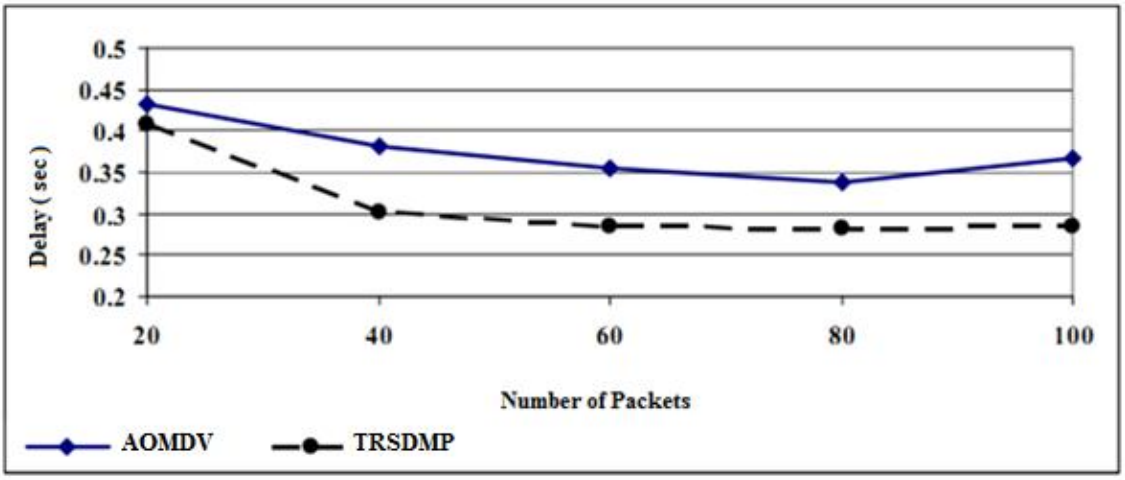

Figure 2. Average End-to-End delay Vs. Number of Packets

The Figure 2 compares between the average end-to-end delay of TRSDMP and AOMDV while changing the traffic load. TRSDMP chooses the set of multipaths with fewer constraints than AOMDV, which causes a reduction in the delay. This, in turn, reduces the delay needed by the source to identify a new path if the existing path becomes invalid or broken. According to this experiment, the improvement ratio of delay reduction gained by TRSDMP is 19%.

Figure 3 shows the discovery overhead of the two protocols as the traffic load increases. TRSDMP has a lower discovery overhead than AOMDV because by using TRSDMP there is a greater number of the discovered paths than with AOMDV. The improvement ratio of discovery overhead reduction gained by TRSDMP in this experiment is 4%.

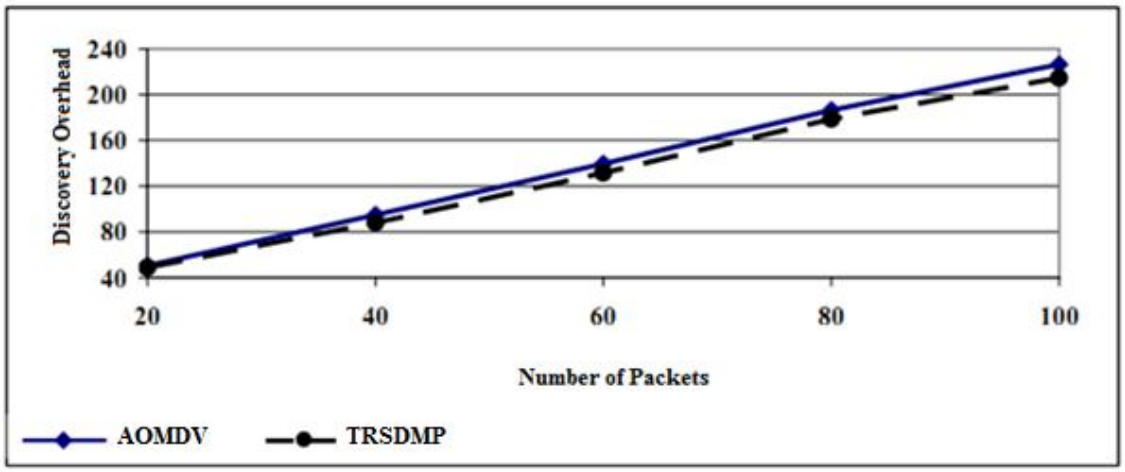

Figure 3. Discovery Overhead Vs. Number of Packets.

The comparison of throughput for the two protocols is shown in figure 4. The improvement ratio of throughput gained by TRSDMP is 3%. The throughput of both TRSDMP and AOMDV decreases as the traffic load increases. This is because when the traffic load increases, the nodes in the network will be overloaded, which obliges them to drop packets.

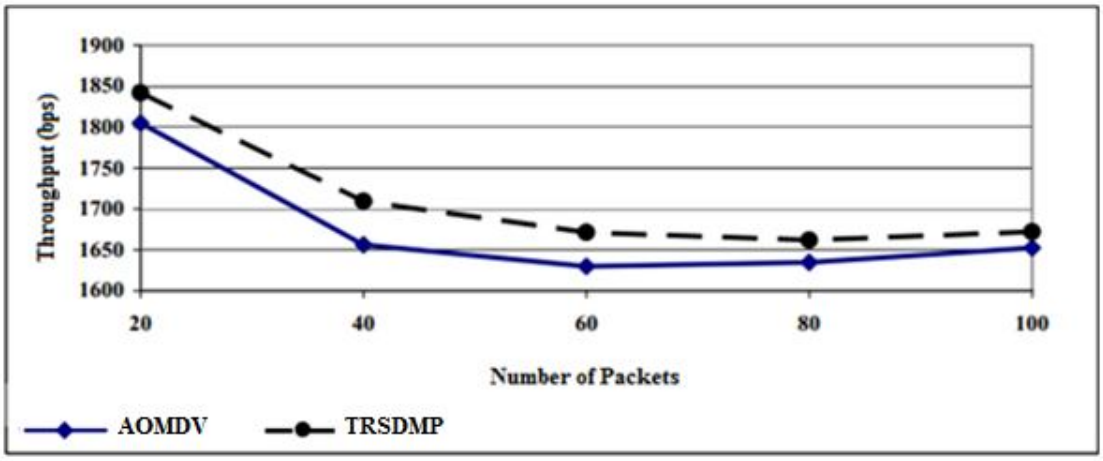

Figure 3. Throughput vs. Number of Packets.

4.2. Density of Nodes

The node density is considered as the performance parameter in the evaluation of the two protocols. In order to change the density of nodes in the simulated terrain a gradual increment of the terrain area was conducted in order to move to a sparser mode. The successive experimental scenarios assume a terrain with a side length ranging from 500 to 3000 metres. In Figure 5, the end-to-end delay of TRSDMP and AOMDV are compared while changing the node density, which is expressed by using the length of the terrain side. In contrast to AOMDV, TRSDMP chooses parted disjoint paths based on the trust level of the nodes. Choosing partially disjoint paths increases the number of selected multipath, and, consequently, decreases the delay resulting from the extra time needed to discover a new path when the existing path becomes broken or invalid. The improvement ratio of delay reduction gained by TRSDMP in this experiment is 9%.

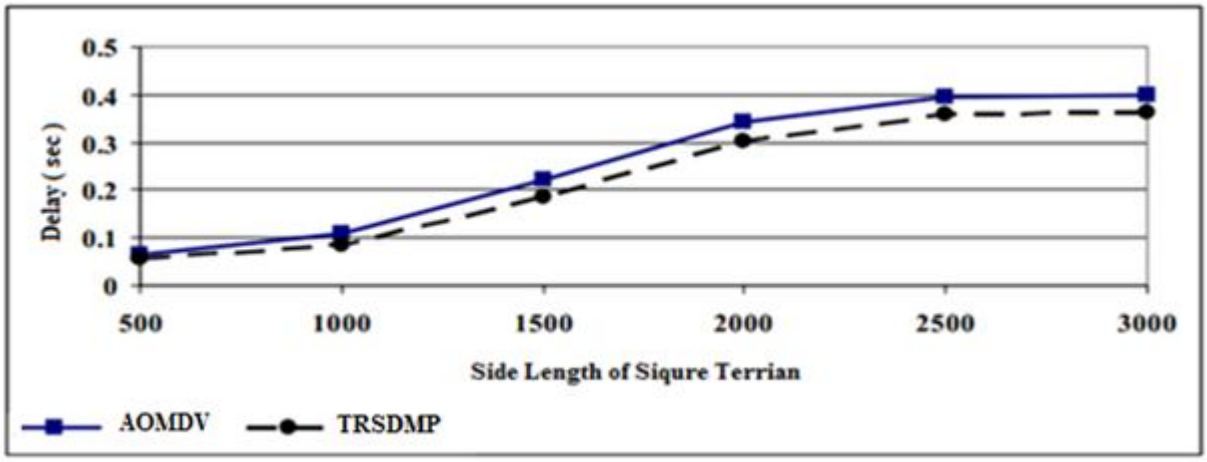

Figure 5. Average End-to-End Delay vs. Terrain Dimension.

4.3. Maximum Number of Allowed Paths

To increase the maximum allowed number of multiple paths that can be stored in a source to a specific destination, we started from two paths since we are interested in multipath routing. The number of paths increased to six paths. In figure 6, we can see from the figure that TRSDMP. Incurs less end-to-end delay than AOMDV with an improved ratio of 4.5%. This is because, TRSDMP chooses not only the maximally spatially disjoint multipath, but also the paths that could partially join at the trusted node.

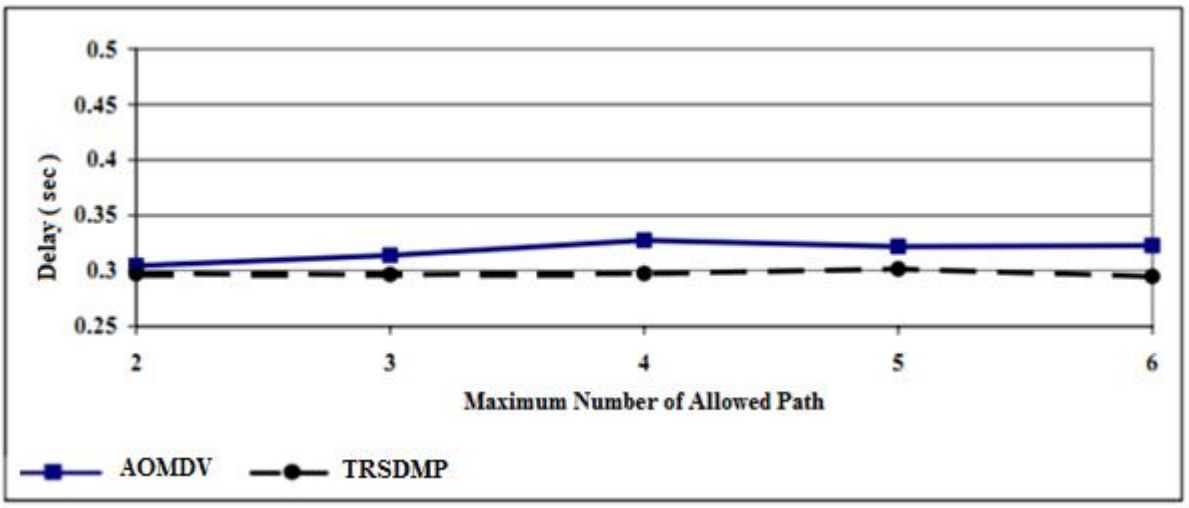

Figure 6. Average End-to-End Delay vs. Maximum Number of Allowed Path.

Choosing multipath based on these criteria increases the number of selected paths that could be used to send data packets. Sending packets over a greater number of paths reduces the average end-to-end delay in case of path breakage.

5. Conclusion and Future Works

In this paper, we have proposed the TRSDMP routing protocol, which chooses the most spatially disjointed paths that could join to a partially trusted level via nodes that specify a certain security threshold. TRSDMP exploits a trusted node to participate in the selected set of routes between a source and destination. The simulation results have shown that the TRSDMP obtains higher throughput than AOMDV under different network conditions. In addition, TRSDMP incurs less average end-to-end delay and discovery overheads than that of AOMDV. As future work, authors propose to compute the trust level of each node based on the properties of the set of discovering multipath and statistical information about how each of these paths behaves in the network.

References

Argyroudis, P. G., and O'Mahony, D. (2004). Secure Routing for Mobile Ad hoc Networks. *Communications Surveys & Tutorials IEEE,* 7 (3), 2- 21.

Berton, S., Yin, H., Lin, C.. and Min, G. (2006). Secure, Disjoint, Multipath Source Routing Protocol(SDMSR) for Mobile Ad-Hoc Networks, *Proceedings of the Fifth International Conference on Grid and Cooperative Computing* (GCC'06), IEEE Computer Society, Washington, DC, USA, 387 – 394.

Bouam, S., and Ben Othman, J. (2003). Data Security in Ad hoc Networks Using MultiPath Routing. *Personal, Indoor and Mobile Radio Communications, PIMRC* (2), 1331–1335.

Han, I. S., Ryou, H. B., and Kang S. J. (2006). Multi-Path Security-Aware Routing Protocol Mechanism for Ad Hoc Network. *International Conference on Hybrid Information Technology (ICHIT'O6), IEEE Computer Society,* 620-626.

Kim, C., Talipov, E., and Ahn, B. (2006). A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks. *Directions in Embedded and Ubiquitous Computing, LNCS(4097),* 522 – 531.

Marina, M. K., and Das, S. R. (2001). On-demand Multipath Distance Vector Routing in Ad Hoc Networks. *in Proceedings of IEEE International conference on Network Protocols (ICNP),* 14-23.

Mavropodi, R., and Douligeris, C. (2006). Multipath Routing Protocols for Mobile Ad Hoc Networks: Security Issues and performance Evaluation. *in Autonomic Communication, LNCS (3854),* 165 -176.

Meghanathan, N. (2007). Stability and Hop Count of Node-Disjoint and Link-Disjoint Multi-Path Routes in Ad Hoc Networks. *in Proceedings of the Third IEEE international Conference on Wireless and Mobile Computing, Networking and Communications.*

Talipov, E., Jin, D., Jung, J., Ha, I., Choi, Y., and Kim, C. (2006). Path Hopping Based on Reverse AODV for Security. *in Management of Convergence Networks and Services LNCS (4238)* , 574 – 577.

Zapata, M.G., and Asokan, N. (2002). Secure Ad hoc On-Demand Distance Vector Routing. *ACM Mobile Computing and Communications Review,* 6(3), 106-107.