SMPR: A Smartphone Based MANET Using Prime Numbers to Enhance the Network-nodes Reachability and Security of Routing Protocols

Govand Kadir, Torben Kuseler, and Ihsan Alshahib Lami
(Corresponding author: Torben Kuseler)

Department of Applied Computing, The University of Buckingham
Hunter Street, Buckingham, MK18 1EG, United Kingdom
(Email: torben.kuseler@buckingham.ac.uk)
(Received July 25, 2014; revised and accepted Nov. 3 & Dec. 13, 2014)

Abstract

Mobile Adhoc Networks (MANETs) emerge as an effective solution for networking Smartphones to enable wireless communication when other alternatives such as cellular networks are not available, e.g. in rural areas. Available MANET routing protocols are either conservative (reactive protocols, e.g. AODV) to control overheads and so do not have any knowledge beyond neighboring nodes, or too expensive (proactive protocols, e.g. OLSR) on resources for Smartphone based MANET networks. Irrespective, all these protocols have limited protection against threats from malicious nodes in the vicinity. This paper proposes SMPR that enables nodes in the network to gain knowledge about the identity of their neighboring nodes. This is achieved by a process of mathematical factorisation of prime numbers performed during the route discovery process. The gained knowledge about their neighboring nodes addresses is then used to validate the participating nodes during data transmission. SMPR is a thin layer code slotted on top of the used MANET routing protocol. Simulation results using OPNET and AODV prove the advantages of SMPR and show that the introduced performance overhead is negligible.

Keywords: AODV, MANET, prime numbers, smartphone networks

1 Introduction

Current mobile devices like Smartphones can handle many networking communication methods (e.g. cellular 2G/3G/4G, Wi-Fi, Bluetooth, NFC) whilst users are on the move. MANETs can be setup between Smartphones easily as no infrastructure is required. This is especially helpful in rural or disaster areas, where infrastructure-based networks (e.g. cellular) are not available. Rescue teams in disaster scenarios, remote scientific missions or ramblers, who want to communicate with each other, can also benefit from this type of networking. However, MANETs lack important secure network requirements like identity of all connected nodes and security of the data communication. This is because any device can join a MANET and MANET routing protocols have limited capabilities beyond establishing communication within the signal range.

To get over these limitations, devices normally rely on information collected about other nodes identity during previous communication, or through the knowledge made available by others inside the network, to achieve "trust" in nodes joining the network. This simple "trust" model is not sufficient when the presences of many security threats that can forge or misuse this information are considered. Moreover, protection for both: a) the route discovery process, and b) all subsequent data transmissions should be kept in mind, too.

In general, MANET routing protocols can be classified into two main types (i.e. proactive and reactive) based on the timing of route discovery. A third class (hybrid) combines algorithms of the other two types [7]. Proactive routing protocols, e.g. OLSR (Optimum Link State Routing), establish routes amongst present nodes in the vicinity prior to any data transmission. These routes are stored in tables and exchanged between nodes regularly, which allow establishing data communication routes quickly. A drawback of proactive protocols is the large overhead to maintain up-to-date routing information about the nodes, which makes proactive protocols not useful in larger networks of mobile devices. The required overhead would drain the resources and battery of these devices rapidly. On the other extreme, reactive routing protocols establish connectivity on demand, whenever a node has data to transmit. The source node floods the air with route requests in an attempt to find a route to the destination. This flooding is propagated via other nodes until it reaches the desired destination. The destination then

sends a traced route reply back to the source. As an example of such reactive protocols, AODV (Ad-Hoc ON Demand Distance Vector) introduces only little overhead but requires much longer establishing a route compared to proactive protocols. In addition, both protocol types do not provide any knowledge about the network structure beyond neighboring nodes. This is a major cause for delay and can introduce security vulnerabilities [1].

Our literature survey (cp. Section 2) of enhancements to reactive and hybrid protocols to overcome these vulnerabilities without adding the overhead of reactive protocols has concluded that prime number algorithms can be a good candidate for improvements. We have further concluded that a proper implementation needs to be a thin crossover layer sitting on the top of any existing reactive protocol controlling the authenticity of the participating nodes without altering the functionality of the protocol itself. This allows using the protocol enhancement with any protocol without the need to alter the protocol implementation or standard. Therefore, SMPR bases on passing Prime Product Numbers (more specifically PPN1 and PPN2) of nodes prime IP-addresses between the nodes during route discovery. This shall provide higher security and better operation especially in larger networks, with only small overhead added to the routing protocol. AODV is chosen to prove our SMPR implementation, but any other reactive protocol [11] could also be used.

The proposed SMPR algorithm bases on the well-known mathematical concept of factoring prime numbers. For this purpose, we use IP-addresses that have a unique prime host part as the ID as further explained in Section 3. In this paper, we introduce the design and implementation of SMPR algorithm in detail and compare its performance with the standard AODV routing protocol.

The rest of this paper is organized as follows: Section 2 presents the literature review. Section 3 explains the SMPR algorithm, while Section 4 details the implementation of SMPR using the OPNET Simulator for various scenarios. Section 5 discusses and analysis the simulation results. Finally, we conclude on the SMPR performance and identify future work in Section 6.

2 Literature Review

Performance and security of MANET routing protocols grabbed the focus of many researchers. Reliability improvements in terms of data integrity and transmission accuracy, as well as reducing the communications overhead (i.e. processing time and resource power usage) were proposed. For example, AODV has the advantage of adding very little overhead to mobile nodes with their limited resources and heavy routing duties. However AODV lacks the knowledge about the transmission path node addresses beyond the next neighboring node, which may cause a security threat to the entire MANET routing protocol. Yet, adding extra knowledge of other nodes identity in the network, as in the OLSR, results in large processing time and power consumption overhead. Therefore, secure/unique identification, location information, and energy consumption are some of the targeted areas for current research, resulting in various enhancements to MANET protocols.

A prime numbers based scheme that helps avoiding malicious node attacks during route discovery by using a clustering mechanism with elected heads has been recently proposed [3]. Nodes have unique prime IDs stored with the cluster head ID in a special table that is used to validate any intermediate node that wants to forward data. The cluster head supports the source node to check the validity of the Prime Product Number (PPN) and decides the trustworthiness of the node. However, trust obtained from previous experience during data transmission is used to decide the trust factor of nodes. Nodes inside the network then pass around this trust to other nodes. This limits the ability to check the trust information passed on by other nodes and as a result, malicious nodes can pass on misleading information about trust factors.

On another vain, prime IP-addresses were used to eliminate nodes enquiry for duplicate IP-addresses by using a prime-DHCP [6]. This eliminates the need to check duplicate addresses and increases the performance by reducing the overhead and latency. Experimenting with this algorithm proofed the concept of prime IP-addresses to be useful for SMPR. Experimental results indicated that SMPR performance can be enhanced by reducing the used prime number to be the host part of the IP-address only. This will minimise the calculation overhead because the calculated PPN values will increase slower as the prime IP-address values are smaller. This avoids extra computational load on any of the involved nodes, especially in larger networks.

Furthermore, prime number based keys are used to secure the nodes ID in MANETs by using a "bilinear paring signature scheme" to reduce attacks [4]. These prime keys act as public keys and sign the RREQ and RREP messages with private keys generated by each node. However, signature based solutions are generally implemented in higher layers, which leads to extra overhead and delay. Such routing algorithms can be further enhanced to use the same prime IP-based keys from the route discovery stage to reduce attacks during the data transmission stage.

It is evident from the reviewed literature that solutions using unique IP-address mechanisms can provide knowledge beyond neighboring nodes. This will enable reactive protocols such as AODV to be more secure and reliable with a negligible introduced overhead.

Location information provided by GPS enabled nodes in a MANET can reduce the overhead of the flooding process during route discovery [5]. This is achieved as nodes can now predict the direction of the destination node and are able to drop RREQ messages passed on to the opposite direction or far away from the destination node. Doing this dynamically by directing messages in a tri-

angle shape and allowing expansion in case of failure to find a destination will improve the AODV performance and reduce the delay. However, this has major security issues, because GPS information passed around can be forged or falsified. We believe integrating GPS information with prime numbers can offer major advantages for both a) securing the route and data communication, and b) reducing the routing overhead.

Power and energy resources are also critical factors in MANET operation, as most mobile nodes are battery-powered devices. Therefore, extra networking activity caused by selfish and uncooperative nodes in MANETs, or caused by added authentication processes during the route discovery or data communication will drain their battery faster. Therefore, algorithms that consider battery power in the route discovery and/or offer added protection with minimum overhead as part of route discovery (which is one of the main ideas behind the proposed SMPR) are desirable to save energy and minimise disruption. To enhance the energy usage, a consumption reputation system can be used [9]. This system checks the energy level of nodes and passes information around using a signature-based scheme. This prevents time synchronisation problems, and extends consequently the lifetime of MANETs but adds extra processing and overhead to the nodes, too.

3 SMPR Algorithm

AODV relies on the routing table to obtain information about other nodes identity in the network when a packet arrives. During a route request (RREQ), AODV stores information about the previous node address (i.e. the node that has send the message), and uses this information later to forward the route reply (RREP) back to the original message source. In addition, AODV stores the address of the sender of the RREP message as the next node address in its routing table. These two addresses are then used during the following data transmissions between the source and destination node of the now successfully established communication route. However, relying on stored information is a potential security concern as malicious nodes may have passed wrong address information around with the aim to interrupt the data transmissions between genuine nodes [12].

To overcome this problem, the proposed SMPR adds a thin check-up process on the top of AODV to force each node in the network to use an address from a mathematical formula rather than relying on a stored address from its routing table. It is important to notice that the SMPR algorithm does not intervene in the functionality of the underlying routing protocol. It is therefore possible to use SMPR with other reactive protocols like DSR, too.

The SMPR algorithm consists of two steps; the first step is executed when a RREP message is received. The second step executes during the subsequent data transmissions. In both steps, PPN1 and PPN2 values

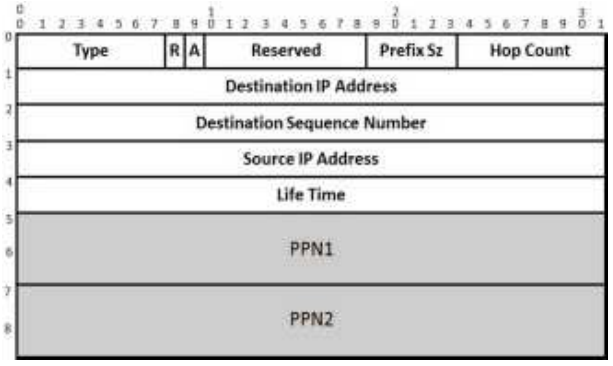

Figure 1: Extended AODV route reply (RREP) header

are used to verify the identity of the involved nodes. The core functionality of these two PPN values depends on the following mathematical factorisation formulas [2]:

Nodes: $p_1, p_2, p_3, \ldots, p_n$

$$PPN1 = p_1 * p_2 * p_3 * \cdots * p_n \quad (1)$$

$$PPN2 = (p_1 - 1) * p_2 - 1) * p_3 - 1) * \ldots) * p_n - 1) \quad (2)$$

$$Factors = GCD(PPN1, PPN2) \quad (3)$$

PPN1 (1) represents the multiplication product of prime numbers, where the pi-values are the host part of the prime IP-address of node i. PPN2 (2) represents the previous PPN1 value minus one, and allows back-tracking the original order of the factors by the receiving node. The greatest common divisor (GCD) value of PPN1 and PPN2 finally represents the factorisation of all values (3) and determines the sequence of nodes inside the path to the desired destination.

3.1 SMPR Implementation

The calculated PPN values are stored inside the individual nodes routing table as part of the SMPR thin layer implementation and passed on between nodes using RREP messages. To enable this, two new 64-bit fields containing the PPN1 and PPN2 values are added to an AODV route reply header as shown in Figure 1.

3.2 SMPR operation

Considering the following scenario in Figure 2, where nine nodes form a MANET network. To enable the sending Node S to establish an entire PPN-based route, the following conditions must be met: a) these nodes must not have any previous communication record, b) the AODV "destination only flag" is set on all nodes, and c) "gratitude reply" must be disabled. If "gratitude replies" are not disabled, then any intermediate node (e.g. node N) that have a path to the destination responds with a "gratitude reply" to the sending Node S that relies on routing table information. This should be prevented as the Node S

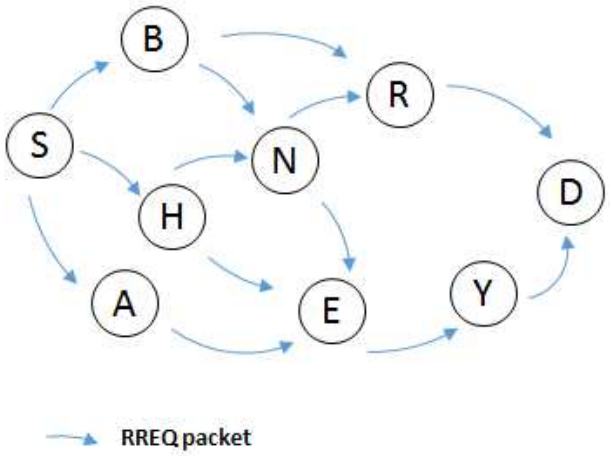

Figure 2: Route request (RREQ) flooding

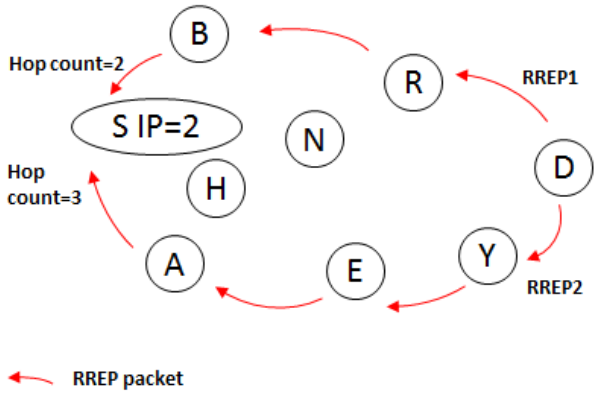

Figure 3: Route reply (RREP) message from Node D to Node S

would not have a full SMPR-based path to the destination in that case.

As mentioned earlier, SMPR does not interfere in any AODV operation. All original AODV route discovery steps are executed normally as detailed in the following paragraphs.

Route Request (RREQ). SMPR is not involved in the broadcasting process of RREQ messages. In the above example of Figure 2, the source Node S holds data that it wants to transmit to the destination Node D. To enable successful data transmission, S creates a RREQ message and broadcasts the message to all nodes that are in transmission range. Once a node receives a RREQ message from one of its neighbors, it compares the destination address to its own IP-address. If they are the same, then the node creates a RREP message. Otherwise, the node will rebroadcast the RREQ. This process continues and the RREQ spreads out inside the network until the RREQ reaches the destination node.

Route Reply (RREP). Once the RREQ has reached its destination, the RREP process starts. The destination Node D creates a RREP message and sends it back to the node from where it has received the RREQ (in our example node R as shown in Figure 3). In addition, Node D keeps a record of node Rs prime IP-address in its routing table to be used in the later data transmission stage to forward data packets.

Once node R receives the RREP, it extracts the destination address (i.e. the originator of the RREQ) from the RREP and compares it to the source address of the RREQ inside its routing table to find the node address where it should forward the RREP to. Node R then adds (or updates it if already exists) the senders IP-Address in its routing table and forwards the RREP to node B. This process continues until the RREP reaches the source Node S.

It is important to note that D receives the RREQs from both nodes, Y and R (cp. Figure 2). Therefore, it creates two separate RREP messages and sends them via the two different paths. This is useful to establish an optimal route as the source Node S can decide later based on the lowest hop count, which route to use for subsequent data delivery. In our example, Node S chooses the RREP route with a hop count of two, i.e. path "S → B → R → D" as shown in Figure 3.

SMPR follows the above-described procedure of AODV with the addition of the following PPN-related steps and calculations.

1) The destination Node D starts the additional SMPR calculations by extracting its own IP-address host part p_{own} (i.e. "11" as shown in Figure 4) as well as the previous nodes IP-address host part p_{prev} (node R with address "5"). Please note that p_{prev} is known to Node D because D received the RREQ from that node.

2) Node D calculates the two PPN values as follows:

$$PPN1 = p_{own} * p_{prev} = 11 * 5 = 55 \quad (4)$$

$$PPN2 = (p_{own} - 1) * p_{prev} - 1 = 10 * 5 - 1 = 49 \quad (5)$$

3) Node D sends the RREP message (cp. Figure 1) including the two calculated PPN values to the next node R.

4) Once the node R receives the RREP, R determines the individual prime factors from PPN1 as described in detail in [2]. PPN2 is used in this calculation to determine the correct sequence of the factor values as PPN1 might have different factor sequences, e.g. PPN1 value of "55" can be factorised as "11*5" or "5*11".

5) Once the factorisation is completed, node R checks if the last value in the calculated factor list is equal to its own IP-address host part, i.e. "5". If this is

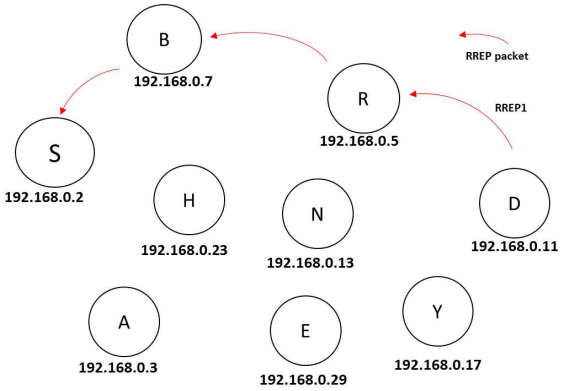

Figure 4: Route for example of PPN values calculation

the case, then the node calculates the new PPN1 and PPN2 values as described before. The only difference is that the node uses the received PPN values instead of its own p_{own} value.

$$PPN1 = PPN1_{rec} * p_{prev} = 55 * 7 = 385 \quad (6)$$

$$PPN2 = PPN2_{rec} * p_{prev} - 1 = 49 * 7 - 1 = 342 \quad (7)$$

6) Finally, node R updates the RREP message with the new PPN values and sends it to the next node, i.e. "B". If the last value of the factor list is not equal to its own IP-address then the node drops the packet. This is to prevent that the node processes a message that is not intended for that node. Lastly, it will store the new PPN values (i.e. 385 and 342) inside the routing table.

7) These steps are repeated by every node inside the path until the RREP message reaches finally the source Node S.

3.3 Data Transmission

In the original AODV, the source node retrieves the data packets from its own buffer and starts the data transmission by sending data to the next node of the previously established route. This next node receives the packet and forwards it to the following node based on the node address retrieved from its routing table. Besides message forwarding, nodes update the expiry time of the particular route entry to avoid that the route will become invalid. This process continues until the data packet reaches the destination Node D as described in Figure 5.

In SMPR, the source node factorises the PPN values to determine the next nodes prime IP-address. The source node then sends the data packet to the next address in the calculated PPN factor list. Upon arrival of the data packet, the next node factorises its own stored PPN, and accepts the packet only if the senders prime IP-address is equal to the number before its own number in the factor list. If this is the case, then the node forwards the packet

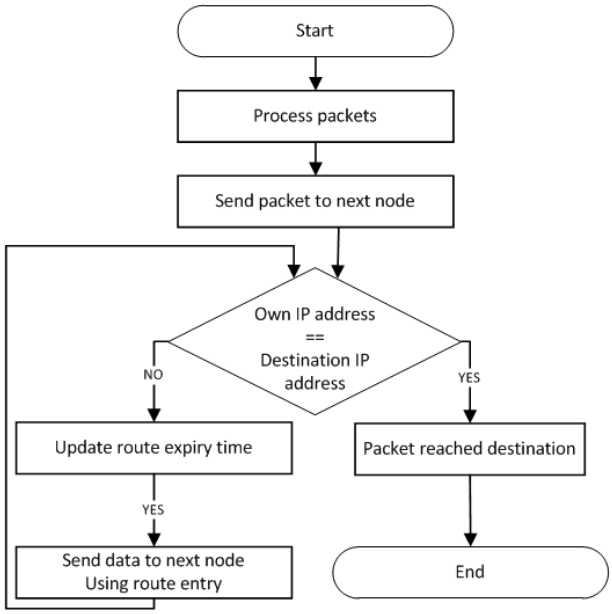

Figure 5: AODV data transmission flowchart

to the next address from the factor list rather than looking for the next address in the routing table. By doing this, SMPR prevents that data packets follow any other path than the path defined via the PPN list. This process continues until the data packet reaches the destination Node D as described in Figure 6.

4 SMPR Implementation

4.1 OPNET Modeller Implementation

SMPR was implemented and tested using the OPNET Modeller [10]. OPNET provides a flexible and highly organised architecture that allows the reusability and extendibility of existing models. OPNET consists of different layers, whereby each layer handles different functionality of the node structure as shown in Figure 7. AODV is a child process of a MANET manager process ("manet_mgr" in Figure 7), which in return is a child of the "ip_dispatch" layer. The added SMPR thin layer is located between the original OPNET AODV implementation and the MANET manager ("manet_mgr").

Integration of this thin SMPR layer requires the following additions and modifications on top of the original AODV process implementation inside the OPNET Modeller:

- Changing the IP-address assignment algorithm to a prime-DHCP algorithm, e.g. [6].
- Adding two extra fields to hold PPN1 and PPN2 in a RREP packet inside the RREP create function.
- Update the RREP send and forward functions to point to values in the PPN factor list, and save the

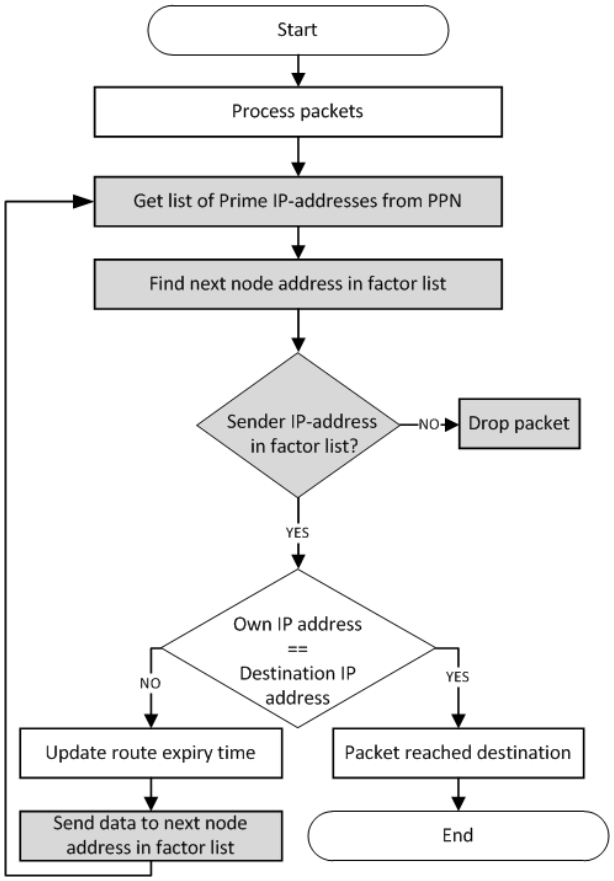

Figure 6: SMPR data transmission flowchart

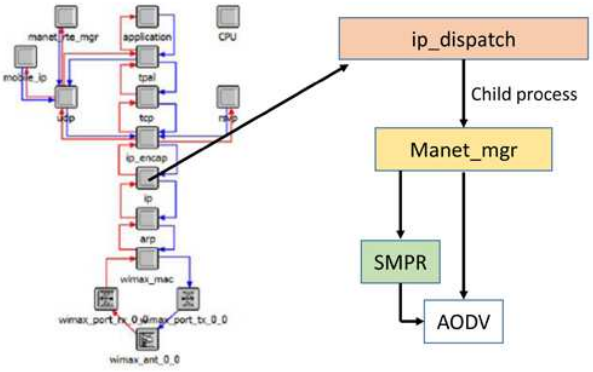

Figure 7: SMPR algorithm inside OPNET WLAN hierarchical architecture

PPN values in the routing table to be used for data transmission.

- Modify the send and forward data packet functions to point to PPN factor values.
- Update the expiry time function to include the PPN values.

4.2 Simulation Setup

Two main scenarios were used to measure the impact of adding SMPR on top of AODV. For each scenario, several node and network characteristics were changed as described below to evaluate the SMPR network performance in terms of introduced overhead and delay:

Node Mobility. Node mobility is defined in OPNET via different configuration parameters like trajectory movement, distance between nodes, and node speeds. Changing these values effects the network performance characteristics like throughput or Packet Delivery Ratio (PDR) [13]. The IEEE 802.11 WLAN standard defines that the distance between two nodes should not exceed 300m. To comply with this condition, the node transmission power in the simulations is set to 0.0005Watt and the packet reception power to -82.65dBm.

Number of Nodes. The network density (i.e. the number of nodes per area unit) has an impact on the network performance, too. A higher network density results normally in nodes having more alternative routes between each other. This can help preventing congestion and can improve the overall performance of the routing [8].

Data Transmission Rate. Mobile nodes feature different data transmission rates and hence, transmission ranges, as describe in the IEEE 802.11g standard. These differences affect the performance of the routing protocol as nodes with a high transmission range might reach nodes that a node with a lower rate cannot reach [14].

In order to assess the effect of the above factors on the performance of our scenarios, the following statistics were collected and evaluated:

Route Discovery Time (RDT). RDT is the time required for the RREQ to reach the destination plus the time required for the RREP to arrive back at the source.

End-to-End Delay (E2E-D). E2E-D represents the time delay that the packet encountered during transmission from the source to the destination.

Packet Retransmission. The average number of packets retransmitted during data transmission.

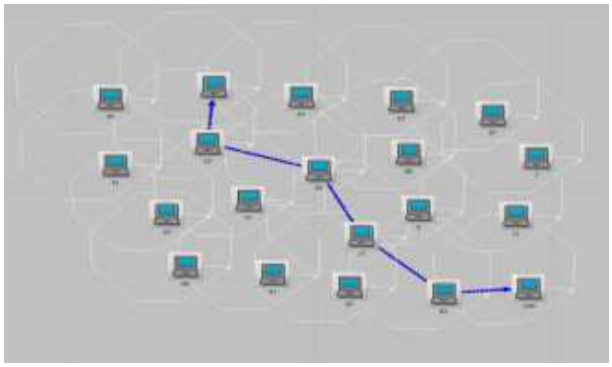

Figure 8: Scenario-I: 20 mobile nodes and their trajectory paths

Two scenarios were used to evaluate SMPR. The first scenario compares the performance of SMPR with normal AODV in a network of twenty 802.11g MANET stations placed in an area with a distance of less than 300m between any two nodes and data rates of 6, 12, 18, 24, and 36Mbps. The simulation considers two nodes sending a data stream in opposite direction as shown in Figure 8. Each transmission will trigger a response back to the sender. Each of these transmissions has an average volume of 500Mbytes per flow. All transmissions are sent concurrently.

The second scenario observes the effect of different node mobility characteristics and network layouts on the performance of AODV and SMPR. This scenario includes 20 nodes placed in five different layouts as shown in Figure 9.

The overall node and traffic characteristics for the first and second scenarios are shown in Table 1.

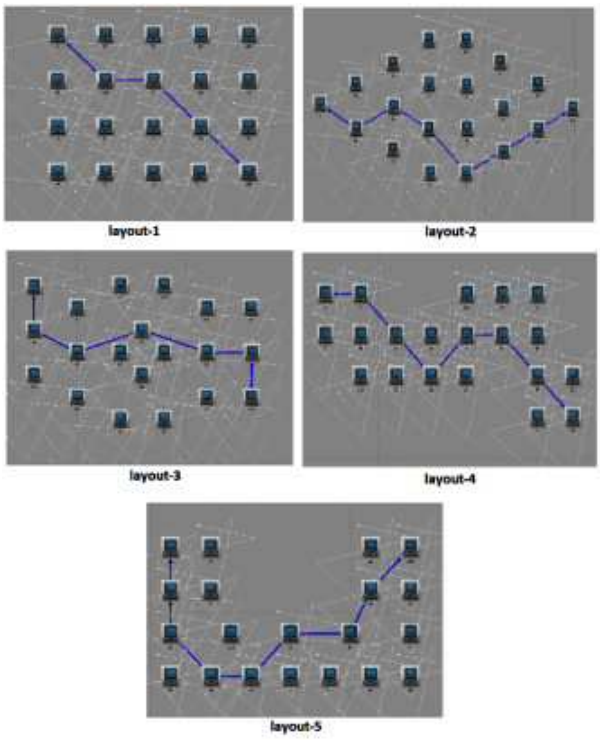

Figure 9: Scenario-II: 20 mobile nodes arranged in 5 different layouts

5 Simulation Result and Analysis

Route Discovery Time (RDT) and Data Transmission (DT) values are used to analyse the collected simulation results and evaluate the effect and performance of SMPR.

Route Discovery Time (RDT) is measured as the average packets round trip time required to successfully receive a RREP from the destination. From the SMPR algorithm design, one can expect that SMPR will introduce a small overhead compared to the original AODV protocol due to the additional PPN values calculations. As can be seen from Figure 10, this introduced RDT overhead is around 0.01msec for data rates of 6, 12, and 18 Mbps respectively. However, this overhead becomes negative for large networks, e.g. for data rates of 24 and 36 Mbps. This is because SMPR already determined the next/previous nodes addresses. Therefore, there will be no need for accessing the AODV routing table to obtain these IP addresses.

The second scenario was further sub-divided into five different layouts as described in section IV.B to evaluate different node setups and network topologies. Table 2

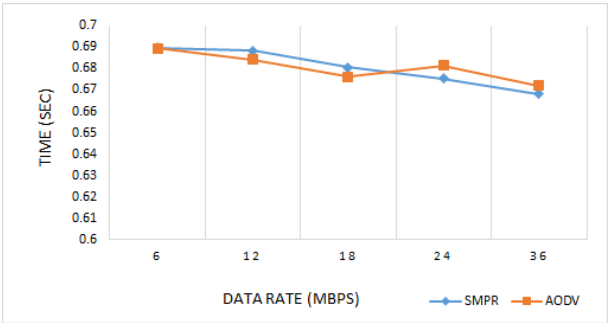

Figure 10: Scenario-I: Route discovery time (RDT)

Table 1: Simulation scenario parameters

Parameter	Value
Trajectory	2 Hexagonal movements: Clockwise & Counter clockwise Movement range: 300m * 300m
Speed	Scenario-I: 2m/s; Scenario-II: 10, 20, 30, 40, and 50 m/s
Distance between two nodes	50, 100, 150, 200, and 250 m (only Scenario-II)
Data rate	Scenario-I: 6, 12, 18, 24, and 36 Mbps Scenario-II: 24 Mbps
Packet interval time variance	1 msec
Node traversal Time	0.04 sec
Packet reception power threshold	-82.65 dBm
Transmission power	0.0005 Watt
Active route timeout	3 sec
Buffer timeout	2 sec
Traffic mix	0.977 GB, all explicit
Simulation Duration	300 sec

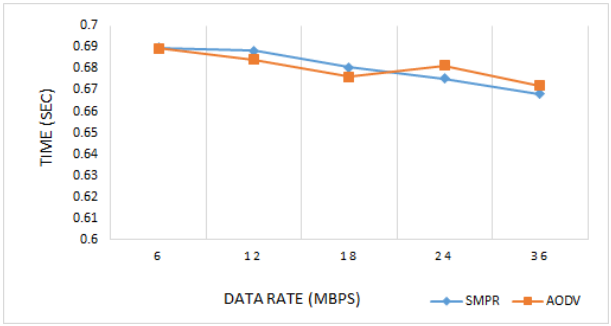

Figure 11: ScenarioII: RDT for the five different layouts

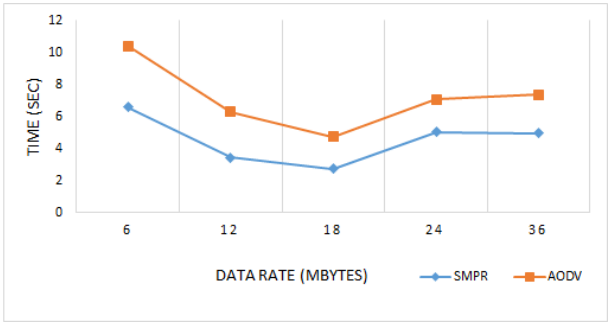

Figure 12: Scenario-II: RDT with different node trajectory speeds

shows the number of hops per route for the five different layouts.

RDT for the first layout is smaller compared to the other layouts as can be seen from Figure 11. This is due to the smaller number of hops in this layout. For the other four layouts, the RDT is very similar as the number of hops is in a similar range, i.e. 6 to 8 hops. In the first layout, SMPR has a slight advantage over AODV (0.453sec RDT compared to 0.456sec for AODV). On average over all five scenarios, SMPR requires only 0.612sec compared to 0.617sec for AODV alone. This is due to the saving achieved by not requiring fetching the IP address of the next node operation.

The nodes speed was the second factor changed to evaluate SMPR. In the simulations, layout-1 was used with five different trajectory node speeds of 10, 20, 30, 40, and 50 m/sec respectively. One can notice from Figure 12 that AODV has a slightly higher RDT compared to SMPR. This is due to the advantage gained by the SMPR factor lists that helps getting the address of the next node faster than accessing this information from the AODV routing table.

The third factor changed was the distance between the different nodes. Layout 1 was used again, this time with a fixed speed. Instead, the distance between two nodes was incremented by 50meters for each simulation. Simulation results show that the RDT increases with increasing distance between any two nodes (cp. Figure 13). This is mainly due to the time it takes the packet to travel on air between the nodes.

Data Transmission (DT) is examined through two statistics: average packet retransmission and end-to-end delay. As mentioned in the scenario setup (cp. Section 4.B), data transmission happens in two opposite directions with the destination nodes sending responses to the source node for each received data packet in the first scenario. These simulations examine the capability of nodes handling different packets in both directions simultaneously. Simulation results show that normal AODV retransmits on average of 7.17 packets compared to an average of 4.65 packets retransmitted using SMPR (cp. Figure 14). This can be explained by the fact that AODV holds only one routing table entry for each route. In our

Table 2: Number of hops per route for simulation II

Layout	Number of hops per route	
	AODV	SMPR
Layout-1	4	4
Layout-2	7	7
Layout-3	6	6
Layout-4	7	7
Layout-5	8	8

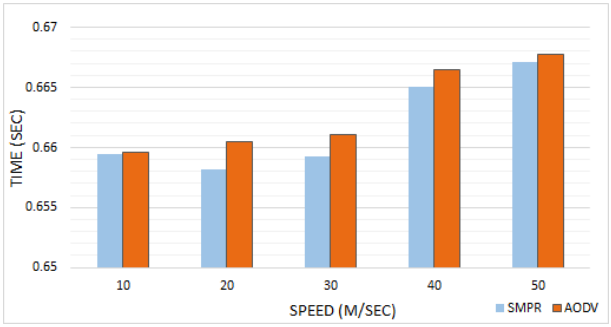

Figure 13: Scenario-II: RDT with different distances between two nodes

Figure 14: Scenario-I: Average packet retransmission

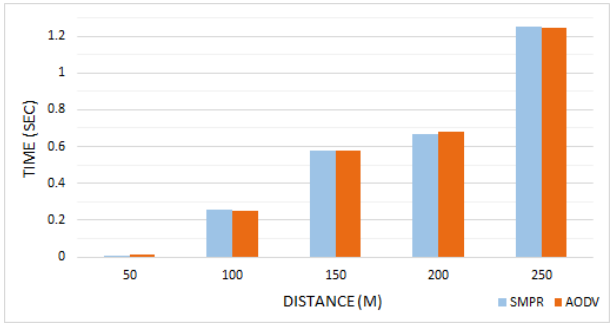

Figure 15: Scenario-I: End-to-End delay

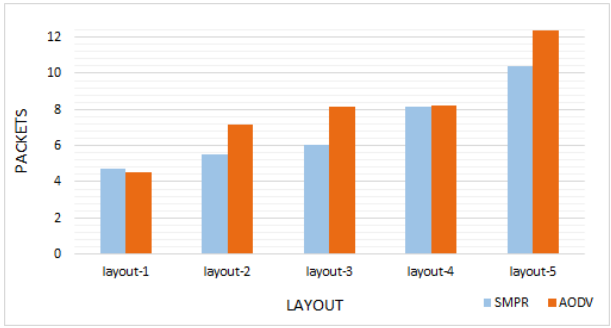

Figure 16: Scenario-II: Average packet retransmission

scenarios, transmissions occur in both directions, which means that AODV needs to figure out the correct direction, i.e. next nodes IP-address from the routing table as there is no check for the senders address. In contrast, SMPR checks the sender nodes IP-address and selects the next nodes IP-address accordingly from the calculated PPN values. As this is faster, SMPR can handle more packets at the same time compared to AODV which results in less packet drops, i.e. packet retransmissions. This clearly shows SMPRs advantage in reducing packet retransmission, as evident in the end-to-end delay times shown in Figure 15 and Figure 17. In scenario two simulation results showed an increase in packet retransmission for the different layouts for both AODV as well as SMPR (cp. Figure 16). This is also due to the increase in the number of hops per route as shown earlier in Table 2.

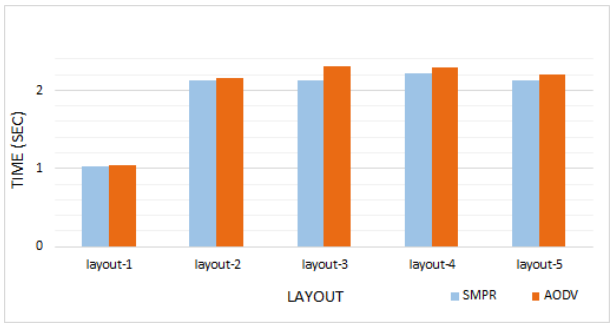

Figure 17: Scenario-II: Average End-to-End delay

6 Conclusion and Future Work

The obtained simulation results clearly show that the implementation of the thin SMPR layer on top of AODV does not introduce a noticeable overhead or delay. Instead, SMPR improves the routing performance by adding certainty about the involved nodes in the transmission, as well as reduces the route discover as well as data transmission time by providing faster access to neighbor node addresses via the PPN lists. It is also important to mention that SMPR helps any node taking part in the communication to gather knowledge knowledge about the identity of nodes beyond their directly neighboring nodes. This information is provided via the PPN factor list and enables the node to identify the direction of packets for two opposite data flows.

Future work will enhance the knowledge beyond neighbors to have the distance between two nodes and the remaining battery power of each node. This will support the source to make crucial decisions about the selected route for transmission. In addition, the algorithm will be enhanced further by permitting already known nodes with prime IP addresses to assign unique identification to newly joined forging nodes that has any IP address and using these IDs instead of their IP addresses. The addition of location information available in wireless enabled devices for example via GPS provides the ability to prevent attacks like wormhole attacks, which is hard to detect when the standard AODV protocol is used.

References

[1] A. K. Abdelaziz, M. Nafaa, and G. Salim, "Survey of routing attacks and countermeasures in mobile ad hoc networks," in *15th IEEE International Conference on Computer Modelling and Simulation*, pp. 693–698, 2013.

[2] A. Al-Sherbaz, *Wimax-Wifi Techniques for Baseband Convergence And Routing Protocols*, Ph.D. Thesis, Applied Computing Department, The University of Buckingham, Aug. 2010.

[3] S. Gambhir and S. Sharma, "PPN: Prime product number based malicious node detection scheme for manets," in *2013 IEEE 3rd International Conference on Advance Computing Conference (IACC'13)*, pp. 335–340, 2013.

[4] U. Ghosh, "Identity based schemes for securing mobile ad hoc networks," in *2012 IEEE 26th International Conference on Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW'12)*, pp. 2514–2517, 2012.

[5] V. Hnatyshin, "Improving manet routing protocols through the use of geographical information," *International Journal of Wireless & Mobile Networks*, vol. 5, no. 2, pp. 19, 2013.

[6] Y. Y. Hsu, C. C. Tseng, et al., "Prime DHCP: A prime numbering address allocation mechanism for manets," *IEEE Communications Letters*, vol. 9, no. 8, pp. 712–714, 2005.

[7] D. Kaur and N. Kumar, "Comparative analysis of aodv, olsr, tora, dsr and dsdv routing protocols in mobile ad-hoc networks," *International Journal of Computer Network and Information Security*, vol. 5, no. 3, pp. 39, 2013.

[8] L. U. Khan, F. Khan, N. Khan, M. N. Khan, and B. Pirzada, "Effect of network density on the performance of manet routing protocols," in *2013 IEEE International Conference on Circuits, Power and Computing Technologies (ICCPCT'13)*, pp. 1089–1092, 2013.

[9] G. S. Kumar, M. Kaliappan, and L. J. Julus, "Enhancing the performance of manet using eescp," in *2012 IEEE International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME'12)*, pp. 225–230, 2012.

[10] Z. Lu and H. Yang, *Unlocking the Power of OPNET Modeler*, Cambridge University Press, 2012.

[11] L. Pal, P. Sharma, and N. Kaurav, "Performance analysis of reactive and proactive routing protocols for mobile ad-hoc–networks," *ISROSET-International Journal of Scientific Research in Network Security and Communication*, vol. 1, pp. 1–4, 2013.

[12] M. Patel and S. Sharma, "Detection of malicious attack in manet a behavioral approach," in *2013 IEEE 3rd International Conference on Advance Computing Conference (IACC'13)*, pp. 388–393, 2013.

[13] R. Paulus, P. D. Kumar, P. C. Philiips, and A. Kumar, "Performance analysis of various ad hoc routing protocols in manet using variation in pause time and mobility speed," *International Journal of Computer Applications*, vol. 73, no. 8, pp. 35–39, 2013.

[14] P. Ramano, "The range vs. rate dilemma of wlans," *Wireless Net DesignLine*, 2004.

Govand Kadir earned his Bachelor of Engineering degree in college of engineering from Baghdad University in 1992. He received his Master of Science degree in Computer Science in 2006 from London south bank university. In 2010, he joined the doctoral program in the Applied Computing Department at The University of Buckingham, UK. While pursuing his degree, Mr. Kadir works since 2007 as a researcher and lecturer for the department of Computer Science and engineering at the University of Kurdistan-Hawler. He is a member of the IT academy sponsored by the council of ministers of Kurdistan regional government of Iraq. Mr Kadir, research focuses on the improvement of routing protocols for Mobile Adhoc Networks and provides protection against malicious devices in these networks. His research is supervised by Dr Ihsan Lami and Dr Torben Kuseler.

Torben Kuseler is a Lecturer in Computer Science and IT Manager at the University of Buckingham, UK. Torben received a Diploma degree in Information Technology with Business from the Applied University

of Wedel, Germany, in 2003 and a M.Sc. degree in Computer Science from the same University in 2005. After moving to the UK., Torben finished his Ph.D. in 2012 at the Applied Computing Department, University of Buckingham, UK. His research focuses on localisation and software protection techniques to enhance authentication security in mobile applications and wireless networks as well as efficient and secure management of Big Data in the cloud. Torben is also the Technical Director of the Dickens Journals Online (DJO: http://djo.org.uk) project, an open access, online edition of the two journals Dickens edited from 1850 to 1870. Please visit http://uk.linkedin.com/in/tkuseler/en and http://www.buckingham.ac.uk/directory/dr-torben-kuseler/ for more details.

Ihsan Alshahib Lami is a Reader/Professor in Computer Science at the University of Buckingham, UK. Ihsan worked in Industry for 18 years designing/managing processor and wireless connectivity chips. His current research teams focus on (1) the hybridisation/integration of GNSS and Wireless technologies for optimum localisation and Smartphone solutions; (2) LTE and Cognitive wireless networks access/security solutions. Please visit http://www.buckingham.ac.uk/directory/dr-ihsan-lami/ for more details.