International Journal of Advances in Computer Science & Its Applications – IJCSIA
Volume 4: Issue 4 [ISSN 2250-3765]
Publication Date : 27 December,2014

Evaluation of Adaptability between QUAD and RZLSR Routing Scheme in MASNet

J.Viji Gripsy, Dr.AnnaSaro Vijendran

Abstract– In recent times, Routing in Mobile ad hoc and sensor networks has provided a challenging and interesting research area due to its impact on numerous science and engineering applications. The principle challenges in MASNETs are frequent changes in network topology, its reliance on battery power and inadequacy of base stations. This research provides a secure multipath algorithm which promotes the nodes in MASNet to execute on-demand discovery by forming set of paths. An Adaptive Secure Multipath Routing (ASMR) is formed with an adaptive behaviour on route discovery and route maintenance phase. In the first phase of route discovery process, in order to obtain efficiency, security and reliability in multi-path routing for MASNETs, propose a routing mechanism, which allows nodes in MASNet to perform an on-demand discovery and generation of a set of paths, based on Dynamic MPR (DMPR) protocol. In route maintenance phase, two algorithms namely QUAD and RZLSR were proposed in a new way using QUAD and RZLSR schemes. In which broadcasting takes place to limited nodes to ensure the time taken to establish a path between source and destination nodes is reduced efficiently. This research investigates the proposed two algorithms with SeMuRAMAS algorithm. Hence, the design of routing protocol should consider the adaptability, security, reachability and its energy efficiency. A set of security mechanisms, based on the utilization of Watchdog and digital signature, are used to protect the route discovery process. The simulation results show that the proposed approach provides notable performance with lesser overhead, energy efficient and better network lifetime.

Keywords: Multipath Routing, Protocol, Security, QUAD, RZLSR, MPR, DMPR, ASMR

J.Viji Gripsy,

Assistant Professor,

Department Of Computer Science, PSGR Krishnammal College,

(Pursuing PhD in SNR Sons College, Coimbatore)

Coimbatore, INDIA.

Dr. Anna Saro Vijendran, Director,

Department Of Computer Applications, SNR Sons College,

Coimbatore, INDIA

I. Introduction

In the last two decades, the importance of routing in MANETs and Wireless Sensor Networks has become an attractive research topic. A number of research works have been carried out to meet out the demands of various science and engineering applications [1]. Due to the increasing demand of wireless communications, a keen impact has been focused on Mobile Ad hoc and Sensor Networks (MASNets) by various industrial and academic communities. The intrinsic features of these networks such as the unreliable nature of links, and the absence of infrastructure, make the networks susceptible to various kinds of attacks [2]. These traits make it tough to exploit the evidence collection techniques and scenarios analysis methods presented in the literature, in order to address digital investigation in MASNets [3]. It is observed from the survey that most of the existing research works have not considered the issue of efficient routing investigation of digital security attacks in the context of wireless networks [4]. In this work, a secure routing protocol which focuses on secure and reliable routing discovery and maintenance process is carried out in MASNets.

This paper propose an Adaptive secure Multi-path routing (ASMR) mechanism, which allows nodes in MASNet to perform an on-demand discovery and generation of a set of paths, based on Dynamic MPR (DMPR) protocol for route discovery process. Then the QUAD based secured multipath routing protocol and Rectangular Zone based Location Specific Routing (RZLSR) protocol for route maintenance which improves the quality of services.

II. Proposed Methodology

The proposed protocol is used to improve the packet delivery ratio from source to destination because it provide an optimal path in terms of bandwidth, automatically due to this the quality of service, throughput and its related parameters of this protocol may be enhanced further. This approach provides a solution for flooding and reduces the power consumption.

III.RouteDiscoveryPhase

This is the mechanism used when S wants to establish a set of paths with DM. Route Request datagrams, say RReq, are sent by S when it does not already have a route to DM. The entirely on-demand properties allow an Adaptive secure Multi-path routing (ASMR) to minimize the overhead and

specify the path-disjointness threshold value. After receiving list of potential paths, S computes all paths to the destination which satisfy the specified threshold, chooses the list of paths to be used, caches the remaining ones, and starts sending the data. Keeping information regarding unused paths allows the reaction to routes modification to be rapid and decreases the overhead related to the generation of a new RReq.

In Multipath DSR, generally HELLO message aids in discovering neighbours. It is send periodically by a node to determine its one-hop neighbours. They are generated and transmitted to all one-hop neighbours to achieve link-sensing, neighbour-sensing, two hop neighbour-sensing and MPR selector sensing. Two-hop HELLO message allows each node to maintain two up-to date lists, first list contains one-hop neighbours and second list contain 2-hop neighbours as detailed in [7]. Nodes in the network maintain list of all nodes that are reachable via symmetric neighbours in the routing table. It helps in MPR calculation. The nodes that have been selected as MPR are informed through HELLO message.

A. Dynamic MPR (DMPR)

An MPR node present in the network is identified by means of MPR computation algorithm. Each MPR node holds a list of 1-hop and 2-hop neighbours. It executes DMPR algorithm before it starts broadcasting. In general, when a node receives RREQ its hop count (hc) value is improved [9, 10].Based on nhc value, the proposed algorithm places constrain in flooding process. On receiving RREQ message, each MPR node checks whether its Hc value is less than or equal to 6, if so unconditional broadcast is carried out to its neighbours. Once hop count value go beyond 6 then route cache of each MPR(x) is searched for Ds, if it is known that the broadcasting is completed by this MPR(x) to its neighbours. In case if there are no Ds in any of the MPR(x) then nhc value is incremented and DMPR algorithm is called recursively till destination is reached.

Algorithm: Dynamic MPR

```
DMPR(MPR(x))
{       static int nhc=6;
   for (each MPR(x))
      if(hc<=nhc)
         Broadcast to its neighbors;
      else
      {  MPR_GC=0;
         for (each MPR(x))
            if (Ds is in x route cache)
               Broadcast to its neighbors;
            MPR_GC=1;
         end for
         if (MPR_GC==0)
            nhc++;
         DMPR( ); }
   }
```

Figure 1: Proposed Dynamic MPR Scheme

In MPR scheme, certain nodes are chosen for broadcasting while it takes place in all the direction. Whereas, in the proposed algorithm it is not only selects few nodes however also restricts the direction of broadcasting. If Ds are identified on a node, DMPR initiate broadcasting only in that region. Reduction in number of RREQ sequentially imposes reduction in routing load. Once the broadcasting is ended source node consist of multiple routes that have been obtained based on threshold value for reaching destination. Source node chooses the shortest path and start forwarding the packets.

IV. Route Maintenance Phase

In this phase, an Adaptive secure Multi-path routing (ASMR) mechanism is proposed here based on QUAD and RZLSR protocol to reduce the link error and also to improve the network security. This is the mechanism used by intermediate nodes to let S update the list of paths in use when the network structure changes or some routes are broken down owing to an attack or sleeping cycles of nodes. This mechanism is based on letting middle nodes bring into play the watchdog concept for every packet and they forward to detect the identities of misbehaving nodes or detect routes errors. If the next hop appears to be broken down, a route error packet, say RErr, is generated and sent to S with the intention to decrease the number of possible path to the destination. The S will consider all the path as broken and endeavor to use another route that goes over the non-responding stored in its cache, which allows to maintain the DPRM. If none backup route to DN is in the cache, the source node invokes again the Route Discovery mechanism.

A. QUAD Based Adaptive Secured Multipath Routing Protocol (ASMR) for Route Maintenance

The proposed routing algorithm imposes the route discovery process and maintenance in conjunction with LAR [14] and ASMR. Six kinds of datagram

are used by QUAD throughout the route discovery in [13]. The function of LAR in QUAD implants the location information and timestamp of each node to its neighbours. In that way source node can identify the location of destination node regarding the route cache. LAR with directional antenna can reduce the routing overhead and recommend effectiveness. The general thing is considered here which has found less influence on conventional method. By this way, QUAD scheme is used to reduce the broadcast region and speedy the process of path establishment.

QUADLNSAlgorithm

```
//LimitingNetworkSpacethroughQUADbroa
dcastingscheme
QUAD_LNS(NetworkSpace,SN,DN)

{Findcenterpointofthenetworkspaceandradius;

    Classifythenetworkspaceintoquadformat
    Ql,Q2,Q3,Q4;Evaluatetheregionofsource
    anddestinationnodes;

    If (SN_Region = DN_Region)

    {IILimitingthenetwor
    kregionLm_Region=
    SN_Region;Return
    theLm_Region;}

// if
SN_RegionisadjacenttoDN_Regio
neitherwayElseif(SN_edge=DN_
edge)

{ //Mergingofselectedregions

    Lm_Region=SN_Region+D
    NRegion;Return
    theLm_Region;}

Else

{
    PredictthedistanceofDNfro
    mtwoadjacentquadsofSN;

    //IntermediateRegion

    Im_Region=RegionhasLessdistancetoDN;

    //Mergingofselectedregions

    Lm_Region=SN_Region+DN_Region+Im_
    Region;}}
```

The above proposed algorithm illustrates that network range can be noted from the density of nodes in the network. As a result, it is essential to identify the center point and radius of the network space. The next step involves in slicing the network space based on the availability of information into quadruple format and assigns the region label. Algorithm now triggered to assess the belongingness of SN and DN node's region. If both SN_region and DN_region are same, it returns the Lm_region as SN_region therefore the original broadcasting range is limited to the specific range.

Or else, SN_region and DN_region are compared as adjacent region in either way. If both are adjacent, now the Lm_region trying to merge the SN_region and DN_region and return the Lm_region as limited network space. If the preceding conditions fail, it means that SN_region and DN_region are belongs to opposite direction. Hence, this sequence is not advised to merge; because the center portion of the merging effect will be narrow band. In this situation, the chances of communication between inter-region nodes are nearly impossible. Thus, intermediate region should be formed to avoid such kind of problems. In this case, we have two intermediate regions and the selection of appropriate region is measured in terms of distance function between neighbouring region and DN. Less distance indicates the closeness to the intermediate region. Therefore, SN_region, Im_region and DN_region are merged together as single limited network space.

B. Rectangular Zone based Location Specific Routing (RZLSR) approach for Route Maintenance

The rectangular shaped request zone only implemented. On the other hand, further definitions may be used [15]. For example, it is feasible to remove the available restriction when defining the rectangular region: one side of the rectangle may be made parallel to the line connecting the location of source node S to the previous location of D in figure2

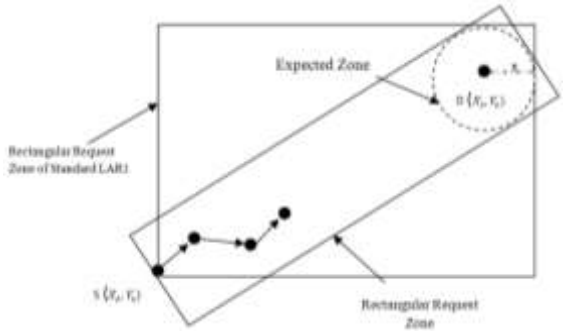

Figure 2: Alternative definitions of request zone: tilted rectangular shaped

In this scheme, the source node S finds out the coordinates of the four request zone vertices. These coordinates are comparative to the plane where the node S is the origin and the x-axis is parallel to the line between S and D. After that, the source translates these coordinates (for the four vertices) to the real coordinates by means of this formula,

$$x = x_1 \times \frac{(y_D - y_S)}{l} + y_1 \times \frac{x_D - x_S}{l} + x_S$$

$$y = x_1 \times \frac{(x_S - x_d)}{l} + y_1 \times \frac{y_D - y_S}{l} + y_S$$

Where (x_I, y_I) are the coordinates of the vertex in the initial plane, and I is the distance between the source node S and the destination node D. Therefore, the coordinates of the four vertices area measured. These coordinates are integrated in the route request packet when commencing the route discovery process. RREQ broadcast is limited to this rectangular request zone. Thus, a node, $I(x_I, y_I)$ forwards the RREQ packet barely when it is in the request zone:

$$\begin{cases} x_I \geq RequestZone.topLeft.x, and \\ x_I \leq RequestZone.bottomRight.x, and \\ y_I \geq RequestZone.bottomLeft.x, and \\ y_I \leq RequestZone.topRight.x \end{cases}$$

Therefore in RZLSR method called (titled rectangular shaped) where the source node S includes the coordinates of the vertices of the request zone within the route request message. To protect the routing algorithm adjacent to forgery of false routing information, a signature based scheme is employed to authenticate nodes and guarantee the integrity of the information they exchange. Suppose, in case of WSN, every node joining the network is authenticated by the BS. Intermediate verification of packets signature permits to remove compromised packets before they reach the destination nodes, which optimizes the used energy and communication resources, and reduces the overhead of the signature verification process performed by the destination node. For the period of the routes establishment, every node generates or forwards the RReq, and adds its identity, the identity of the next receiving nodes, and sur-signs record the route. A node which may receiving the forwarded message confirm whether the final appended signature is correct or not, may checks if it is assumed destination, determines the immediate sender (the neighbor node from which the packet is being forwarded) of that datagram and makes sure that it is a neighbor. In case, it adds its identity, the identity of the feasible next hops and sur-signs the datagram. As an alternative of WSN, signature is performed by means of elliptic threshold signature algorithm is used. In addition, when an intermediate node eliminates a received *RP* list instead of forwarding it, the watchdog mechanism used by neighbor nodes will detect such behavior.

V. EXPERIMENTAL RESULTS

In order to evaluate the proposed protocol, the simulation is carried out using simulator version 2 (NS-2). NS-2 is a famous network simulation tool. Number of nodes in the network is selected to be 50, 100 and 150 for different simulation runs. The nodes are limited in a 1000x1000 m² area. Their primary locations are attained by means of a uniform distribution. Individual nodes move about next in a random waypoint mobility representation as there in [16][6], each node moves incessantly, without pausing at any location.

The performance evaluation is measured by the graphs.

i. Packet delivery ratio (PDR): PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. This metric shows the reliability of data packet delivery. In figure 1, PDR is plotted against the number of nodes.
ii. Packet overhead: The number of transmitted routing packets. For example, a HELLO or TC message sent over four hops would be counted as four packets in this metric. In figure 2, packet overhead has been plotted against number of nodes.
iii. Throughput: This metrics represents the total number of bits forwarded to higher layers per second. It is measured in bps. It can also be defined as the total amount of data a receiver actually receiver to obtain the last packet.

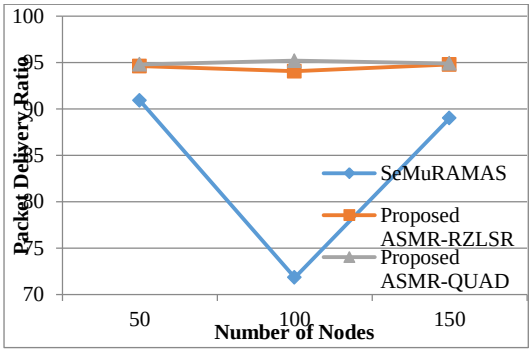

Figure 1: Packet Delivery Vs Number of Nodes

The Figure 1 is drawn for the packet delivery versus Number of nodes. From the figure the proposed ASMR-QUAD system which has high packet delivery ratio when compared with another proposed ASMR-RZLSR scheme and the existing techniques like SeMuRAMAS technique. The results illustrate that the proposed ASMR-RZLSR and ASMR-QUAD has found less difference in the packet delivery ratio compared to SeMuRAMAS. Thus, it can be concluded that the proposed two algorithms were found to have significant impact on packet delivery ratio.

The Figure 2 is drawn for the Throughput versus Number of nodes. From the figure the proposed ASMR-RZLSR system which has high Throughput value when compared with another proposed ASMR-QUAD scheme and with the existing techniques like SeMuRAMAS. The results illustrates that the proposed ASMR-RZLSR approach performs better

when compared with other algorithms like ASMR-QUAD and SeMuRAMAS.

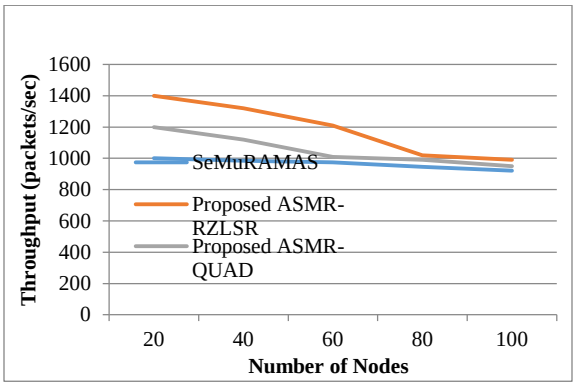

Figure 2: Throughput Vs Number of Nodes

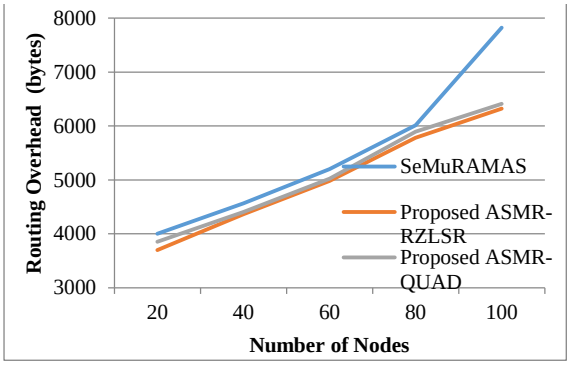

Figure 3: Routing Overhead Vs Number of Nodes

Figure 3 is drawn for the Routing Overhead Vs Number of nodes. From the figure the proposed ASMR-RZLSR system which has low Routing Overhead value when compared with another proposed ASMR-QUAD scheme and with the existing techniques like SeMuRAMAS. The results illustrates that the proposed ASMR-RZLSR approach performs better when compared with other algorithms like ASMR-QUAD and SeMuRAMAS.

VI. CONCLUSION

Wireless Adhoc and Sensor Networks are capable to use multi-path routing, specifying both the number of paths that should be available between a source and a destination, and the maximal number of nodes to be shared by these paths. An Adaptive Secure Multipath Routing Algorithm (ASMR) is developed for Mobile Adhoc and Sensor Networks to make secure route discovery. This research is intended to explore the better adaptability of proposed two algorithms. The simulation result shows that in all the cases ASMR-RZLSR is doing significant performance than ASMR-QUAD. Hence, it is seen that in ASMR which considers both the areas of routing and bandwidth, have DMPR module in route discovery phase and RZLSR module for route maintenance thereby efficiently reducing the time to establish a path between the source and the destination nodes and also reduced the routing overhead.

References

[1] Nicole Lang Beebe, Jan Guynes Clark, A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation. 2, 147–165 (2007)

[2] Slim Rekhis, Noureddine Boudriga, Logic-based approach for digital forensic investigation in communication networks. Computers & Security (2011, in press)

[3] Shuo Ding, A survey on integrating manets with the internet: Challenges and designs. Computer Communications, 31(14), 3537–3551(September2008).doi:10.1016/j.com.2008.04.014

[4] Slim Rekhis, Noureddine Boudriga, A formal rule-based scheme for digital investigation in wireless ad-hoc networks, in Proceedings of Fourth International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering, (Oakland, California, USA, 21 May 2009), pp. 62–72

[5] Anna Saro Vijendran and J.Viji Gripsy, **"**RECT Zone based Location-aided Routing for Mobile *Ad hoc* and Sensor Networks", Asian Journal of Scientific Research 7 (4): 482-487 2014

[6] Oberg, L. O and Xu, Y. (2007) 'Prioritising bad links for fast and efficient flooding in wireless sensor networks'. In proceeding of the International Conference on Sensor Technologies and Applications. October 14-20. Valencia, Spain. Hou, X., Tipper, D., Kabara, J.: Label-based multipath routing in wireless sensor routing. In: Proceedings 6th International Symposium on Advanced Radio Technologies (ISART 2004), Boulder, CO (March 2-4, 2004).

[7] Bayrem Triki, Slim Rekhis, and Noureddine Boudriga, "Threshold Based Multipath Routing Algorithm in Mobile Adhoc and Sensor Networks", Springer, E-Business and Telecommunications, Volume 222, 2012, pp 54-70, 2012.

[8] Gripsy, "Scalable & Secured Route Discovery Mechanism using DSR Protocol", Parallel, Distributed and Network-Based Processing , pp. 619-626, 2011.

[9] Bastian Blywis,Mesut Günes, Felix Juraschek,Oliver Hahm, Nicolai Schmittberger, "A Survey of Flooding, Gossip Routing, and Related Schemes for Wireless Multi-Hop Networks" ,Technical Report TR-NO: TR-B-11-06, 2011.

[10] Ou Liang,Y.Ahmet Sekercioglu, and Nallasamy Mani,"A Survey of Multipoint Relay based broadcast schemes in Wireless ad hoc networks", IEEE Communications surveys & Tutorials, vol.8 , 2006.

[11] Prayag Narula a, Sanjay Kumar Dhurandher,Sudip Misra b, Isaac Woungang "Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing", *Sci. Direct Comput. Commun.*, vol. 31,pp.760 -769, 2008.

[12] J. Viji Gripsy and Anna Saro Vijendran, "QUAD Based Secured Multipath Routing Protocol for Mobile Ad hoc Networks", Information Technology Journal 13 (8): 1505-1513, 2014.

[13] Ko, Y.B. and N.H Vaidya, 2000. Location-Aided Routing (LAR) in mobile ad hoc networks. Wireless Networks, 6: 307 -321.

[14] Shin T. and Yen, H.(2008) 'Location-aware routing protocol with dynamic adaptation of request zone for mobile ad hoc networks'. Journal of Wireless Networks. Vol.14, No. 3, pp. 321-333.

[15] Mohammad AlOtaibi and Hamdy Soliman, "Routeless Routing Protocols over MASNETS: More Energy Saving Approaches, "International Journal of Wireless & Mobile Networks (IJWMN), Vol.2, No.3, August 2010.