Secured Residual Power Aware Routing Protocol for Manets

Joshua Reginald Pullagura, D.Venkata Rao

Abstract: ***The MANETs are a form of wireless communication in which the routing is done via mobile nodes. As these are mobile means they are having mobility nature and there is no static position of nodes. The routing is based on the protocol chosen, there are so many routing protocols for communication. In earlier days the routing is based on traditional protocols which required centralized administration and monitoring. Later on, Mobile Adhoc Networks are evolved which provided users with wireless communication capabilities like dynamic topologies, cooperativeness, scaling of network and infratsructureless capabilities etc. The major challenges in Manets are security and energy consumption. The nodes are operated with the help of energy source so the energy management is a primary concern in network. The routing protocol consists of mobile nodes and scaling of network may allow malicious nodes/ intruder into network. The protocol proposed in this paper takes care of energy management as well as security mechanism. The Secured Residual Power Aware Routing (SRPAR) provides users to choose the path with maximum lifetime and provides session keys to enhance the security aspect. The session key is provided with the use of Diffie Hellman algorithm. It provides authentication and prevents the new node and intruder node to enter into routing without authentication.***

Keywords: MANETs, SRPAR, security, energy, routing.

1. INTRODUCTION

The evolution of MANETs makes the network capable to use in various environments and applications. The MANETs are self healing and self organization networks which make mobile nodes to deploy anywhere in the network and to remove any node in network. The nodes are operated with the help of power source which greatly influences the lifetime of the network. In some cases there is a need of short lifetime path but major of the cases need the network with more active time. As this is the case, there must be a major care about the battery power. The transmission, reception, sending of beacon packets, finding of alternate paths, link failure parameters affect the battery lifetime which affects network lifetime. The applications of MANETs include military sector, disaster recovery, personal area networking, business applications, and so on.The major challenges in MANETs are limited bandwidth, security threats, dynamic topologies, routing overhead, energy constraint etc. If the energy of node exhausts then it leads to link breakage in the network. In this paper the considered challenges to modify are battery power and security threats. To achieve maximum lifetime the routing protocol is designed which maintain routing table and it maintains energy record of all the nodes[9]. In any network there may be more than one possible path for communication. Out of all available paths the route with more life time is selected for routing with the help of energy records in routing table [10]. Secondly the security threat is due to the malicious node or intruder or any new node which is not in the routing table. This is issue is surpassed with the help of key exchange mechanism called Diffie Hellman algorithm. The Diffie Hellman provides authentication in the network it restrict the new nodes to enter into the network in routing phase. The new node may enter into the network but it is possible by recording the node in routing table. The new protocol called Secured Residual Power Aware Routing (SRPAR) is designed to achieve maximum network lifetime and also provides authentication.

2. RELATED WORK

2.1. Routing protocols

The routing protocols are mainly categorized into three types- proactive, reactive, hybrid protocols. The proactive routing provides the routing with the maintenance of routing table with metrics as number of hops, distance between nodes, source address, destination address, sequence number of nodes etc. The possible routes are stored in routing table and provides alternate paths if needed. The major drawback with this routing is periodically it have to update the routing table which consumes more bandwidth. The example of routing protocols is DSDV (Destination Sequenced Distance Vector routing).The reactive protocols provides the route on demand i.e., whenever there is a need then only the route is provided. There is no periodic exchange between the nodes. The reactive protocol consumes less BW, less overhead than proactive protocols. AODV (Adhoc On demand Distance Vector routing protocol) is best example for reactive routing.

The hybrid protocol is derived from both proactive and reactive protocols. This protocol takes advantages of both and provides efficient routing. Zone Routing Protocol is an example of hybrid routing. The above mentioned categories don't take care of energy metric. Later on many energy aware routing protocols [1,3] are introduced which deals with transmission power, receiving power, link failure cost, individual node power, lifetime etc.

2.2. Energy aware routing protocols

The majority of the protocols deal with minimum hop metric but to maximize the network lifetime the energy metric should also be considered. Some of the energy aware

Revised Manuscript Received on February 11, 2019.

Joshua Reginald Pullagura, Vignans foundation for Science Technology and Research Deemed to be University Guntur, AP, India.(pjreginald@gmail.com)

Dr.D.Venkata Rao, QIS College of Engineering and Technology, Ongole, AP, India.

routing protocols are MTPR, EEAODV, MBCR, MRPC. Out of these protocols MTPR is Minimum Transmission Power Routing. This protocol calculates the transmission of all possible paths and selects the path which has minimum power consumption. By this MTPR tries to minimize the energy consumed to forward the data but it doesn't directly affect the network lifetime. The MRPC is Maximum Residual Packet Capacity takes care about battery cost along with link failures. The packet is transmitted properly means it consumes optimal power. If the packet is not transmitted properly then it includes retransmissions which in turn consume more power. In some of the cases link may fail due to movement of node beyond the range or node may exhaust due to lack of energy. So these cases also need to be considered while providing efficient routing. One of the foremost routing protocol is AODV [4] is used in many wireless applications but the limitation with this protocol is it doesn't include energy metric. Later this is modified with energy metric [7] named as EEAODV-Energy Efficient Adhoc On demand Distance Vector routing. In EAODV it maintains the threshold value to provide energy efficient path. For every node in the route it checks the energy level present [8]. If the energy is less than threshold value then the node is discarded and will search for alternate one [9]. If the node energy is greater than threshold level then it is considered to be present in the path. In this way it modifies the traditional AODV. Cluster based [6] approach is one of the widely used scheme in route maintenance process

2.3 Security mechanism in MANETs

The second challenge that considers to optimize in this paper is security. The MANETs are of wireless network means that environment may easily affected by intruder or malicious node. The major security threats in MANETs are availability, confidentiality, integrity and authentication.

The main thing in network is exchanging of information. The availability refers to unauthorizing of resources. The prime constraint is contravened by DoS attack in MANET.

Confidentiality refers that the info regarding the network is allowed to read/ refer/ accessed by authorized user only. This feature ensures that data is protected from passive attacks. Many of the business applications, military related messages and information need to maintain with high confidentiality.

Integrity provides the feature that only the authorized users are allowed to modify the information. Authenticity gives the information about the node whether it is a trusted node or genuine node. Without authentication the network may be affected by malicious node and it may access the confidential information in the network without permission.

The security is provided with the help of key mechanisms, encryption, digital signature etc. The simple and efficient technique to provide security is key mechanism. The Diffie Hellman key exchange is one of the prominent symmetric key exchange mechanism which provides common key to share between the nodes which ensures authentication by not entering the eavesdropper node to obtain a key shared. This was introduced by Whitfield Diffie and Martin Hellman in the year 1976. So in this paper we considered the Diffie Hellman key exchange technique to provide security in the network. With the combination of energy and security metrics a new routing protocol Secured Residual Power Aware Routing (SRPAR) is proposed.

3. PROPOSED METHODOLOGY

Generally in MANETs the routing is provided by considering minimum hops. Even though there are less number of nodes that particular nodes may not have sufficient energy to make the path active upto data transmission, in those cases transmission will fail. This leads to rerouting of the network in turn consumes more energy. So energy consumption is a major criteria. As this is a wireless network there is more chance to enter the malicious node into the network. We have to prevent the new nodes entering into particular route during routing. This is achieved with help of so many security mechanisms. The simplest authentication technique that provide key for the particular session is done with the help of Diffie Hellman algorithm. To avoid these drawbacks, Secured Residual Power Aware Routing (SRPAR) protocol is proposed.

3.1 SRPAR protocol:

The SRPAR is an on demand routing protocol means the route is provided only when there is a need. Unlike above mentioned protocols like MTPR and EEAODV, SRPAR provides the more network lifetime by considering the energy of nodes individually. This consideration provides optimal, active and secured path between source and destination nodes. This protocol follows the max-min strategy while providing the route for transmission by calculation energy of each path.

This protocol starts by route discovery and route establishment. The routing process is similar to EPAR [9] , as it first find out the maximum of minimum node energies using max-min strategy for all the existing paths. Then it finds the maximum energy path from the available paths to transmit data to its destination. The below Figureure 1 shows the protocol, out of the three available paths N1-N5-N6-N7, N1-N2-N3-N6-N7, N1-N5-N3-N4-N7, the path N1-N2-N3-N6-N7 is selected for routing. Since it is having maximum lifetime in the network.Later the nodes in particular path computes the secret key using Diffie Hellman algorithm for exchanging information and then shared between the nodes in the network. In this way optimized and secured routing is possible with this protocol. SRPAR restricts new nodes to enter into the path while routing with the use of shared key i.e., the node which is present in the routing table those nodes are only allowed for routing and key will share among those particular nodes in that path. The protocol description is as follows in detailed manner. After the path selection, the key must be shared between the nodes to achieve security in the protocol. Here the key exchange mechanism is with the help of Diffie Hellman algorithm.

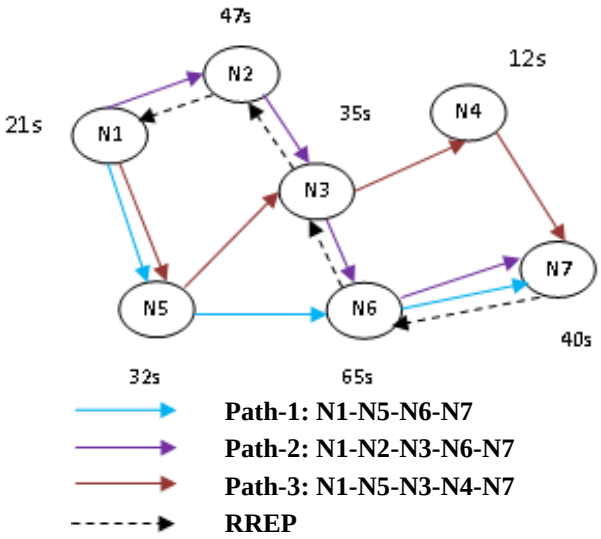

Figure 1. Route discovery and establishment in SRPAR showing different paths and route reply

3.2 Key sharing to the nodes in the path using Diffie Hellman algorithm:

Diffie Hellman algorithm:

The Diffie Hellman is one of the symmetric key agreement mechanism. This provides forward secrecy as well as authentication in the network. While transmission over public network this gives authentication. This technique uses group of integers, greatest prime number, modulo operation and a base to compute the key. Here is an example of key computation:

Let the nodes be N1, N2, N3 and so on

1. The nodes must agree on the chosen prime number, let it be 23 in this and the base is 5.

pn (prime number)=23, bn (base number)=5

2. The first node N1 selects a secret integer (a) to that node as 6, and compute A then send to N2.

$$A=bn^{a} \bmod pn = 5^{6} \bmod 23=8$$

3. The node N2 selects a secret integer (b) to that node as 15, and compute B then send to N1.

$$B=b^{b} \bmod pn=5^{15} \bmod 23=19$$

4. N1 computes secret key sk as

$$sk=B^{a} \bmod pn= 19^{6} \bmod 23=2$$

5. N2 computes secret key sk as

$$sk=A^{b} \bmod pn= 8^{15} \bmod 23=2$$

6. Now the secret key 2 is shared between the nodes as encryption key. The node which is having the key is only allowed for data exchange. Similarly the key is computed for N number of nodes and allow secure communication between the nodes.

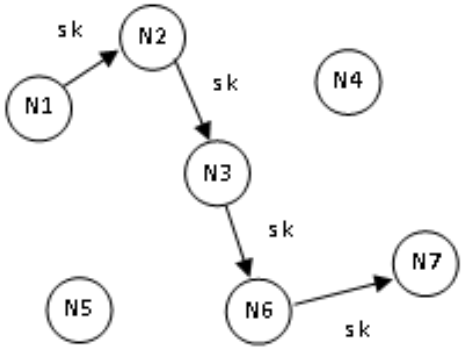

Figure 2. Path in SRPAR showing sharing of key among nodes

The SRPAR provides authentication in the network by avoiding the new nodes to enter into the network. The Diffie- Hellman is a powerful key computation mechanism which provides the key for communication. By this, while routing no other new nodes enters to routing path without authentication. Like this way the security is achieved Tables

3.3 Route maintenance in SRPAR:

The network sometimes may fail to transfer the data due to some reasons. The main reasons for flattening of network is the nodes battery power or node moving out of communication range. This entails link breakage in the network. This link failure sends route error (RERR) packet back to source node. The protocol maintains an assistance node to acts as backup node in case of link failure. By this way the network periodically reforms. Even though the link may fail it will repair in few moments and provides communication.

3.4 Working of SRPAR:

The working of secured EPAR is shown in below flowchart. The following are the steps

1. Initially it broadcast the RREQ and searches for destination node.
2. The intermediate/ destination node sends the reply back to the source node.
3. Determines the minimum hop energy of all available paths.
4. Consider the maximum of all minimum hop energies.
5. Compute the key for data transmission using Diffie Hellman algorithm.
6. Share the computed key with next node.
7. While transmission the node is allowed to enter key.
8. If entered key is matched with shared key then the node is allowed to retriee data and continues with transmission, otherwise transmission is discarded.
9. The same process will continue with every session

4. SIMULATION ENVIRONMENT AND RESULTS

The network simulator-2.35 is used as a simulator in this protocol performance evaluation. The ns2 is event driven simulator and easy to use. The network parameters considered to evaluate the performance are end to end delay,

throughput, lost packets, energy consumed and lifetime of the network. The following table shows the simulation parameters

Table 1. Simulation Parameters

Simulator	NS-2.35
Antenna	Omni directional
Protocol	SRPAR, EPAR, MTPR
Number of nodes	10,20,40,60,80,100
Traffic type	CBR
Mobility model	Random way point
MAC layer	IEEE 802.11

4.1 Performance Metrics :

The Performance Metrics considered for analysis of the three protocols are discussed below.

1. Throughput: It is also stated as packet delivery ratio. It is calculated by taking the ratio the number of packets sent to number of packets received. Figure.3 shows the throughput of the protocols for various number of nodes. The throughput is more for SRPAR compared to MTPR, EPAR Protocols.

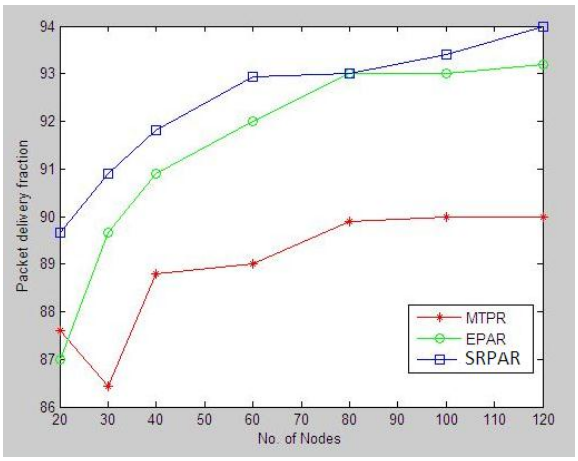

Figure 3. Throughput v/s number of nodes

2. Energy: The energy consumption is the energy used by the nodes in the network to complete data exchanging in the network. Below plot clearly shows that energy consumed for SRPAR is low when compared to EPAR and MTPR.

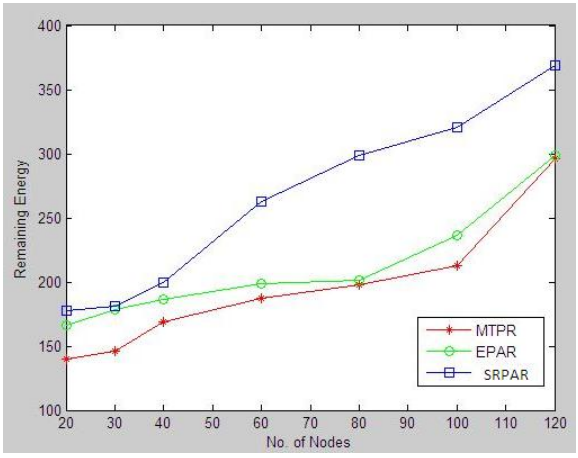

Figure 4. Remaining battery power v/s number of nodes

3. Lifetime: The network lifetime provides how much time the network is active. It is based on the energy consumed by the node. Figure.5 shows that SRPAR has more network lifetime (seconds) while compared to EPAR, MTPR. The lifetime of the SRPAR is slightly increased than EPAR since it involves key computation and sharing.

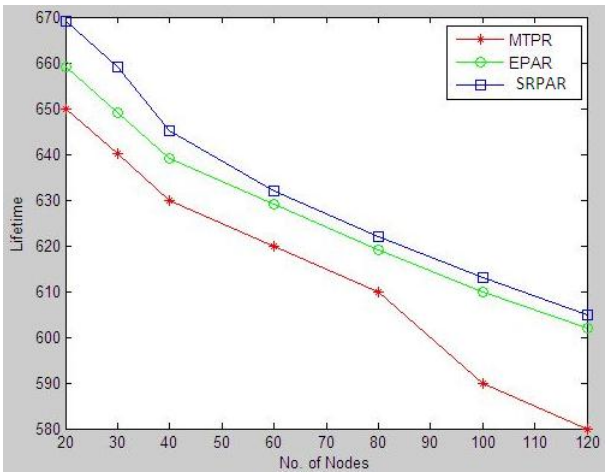

Figure 5. Network lifetime v/s number of nodes

4. Routing overhead: It describes number of routing packets used for communication. It should be minimal for a good routing protocol. The below plot shows the routing overhead for the three protocols. SRPAR shows better performance when compared to other two protocols.

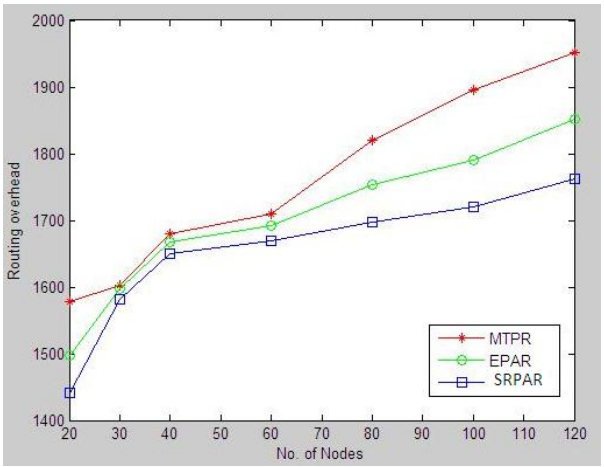

Figure 6. Routing overhead v/s number of nodes

The parameters of the network and comparison between various protocols are shown here in the Table 2.

Table 2. Comparison of network parameters

Parameter	MTPR	EPAR	SRPAR
Throughput (%)	82	85	87
Consumed Battery Power (%)	77	74	72
Lifetime (%)	79	84	85

5. CONCLUSION

In this paper, we analyzed the performance of SRPAR by considering some of the important network metrics. The proposed protocol SRPAR is based on Diffie Hellman key exchange technique and it provides energy efficiency as well. It provides the path by considering energy metric in routing table. The Diffie Hellman provides authentication in the network and it restricts the new node entering into the path without proper authentication. At first the energy optimal path is selected and then key is computed for the nodes in the network. The key is computed with Diffie Hellman algorithm and then it is the shared between the nodes in the path. The node which has key is allowed for exchange of information. SRPAR provides energy optimization and security with the help of key management scheme. The performance of SRPAR when compared with other energy aware protocols like MTPR, EEAODV shows better performance.

REFERENCES

1. Nandkishor M.Pawar, Nandkishor P.Karlekar, "*A survey on energy efficient routing protocols in MANET*", International Journal of Computer Science and Mobile Computing (IJCSMC), ISSN 2320-088X, Vol.3, Issue. 12, December 2014, pg.133-139.
2. P. Sathya Priya, Seethalakshmi.V, G.Mohan Kumar, "*Efficiency enhancement of energy aware ad hoc routing protocols*", International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC) ISSN 2250-1568, Vol.3, Issue 1, Mar 2013, 209-220.
3. Dharam Vir, S.K.Agarwal, S.A.Imam, Lalit Mohan, "*Performance analysis of MTPR routing protocol in power deficient node*", International Journal on AdHoc Networking Systems(IJANS), Vol.2, No.4, October 2012 DOI:10.5121/ijans.2012.240767.
4. Heena Mital, Lokesh Kumar, "*Research paper on hybrid model of AODV & MTPR for MANET*", International Journal of Enhanced Research in Management & Computer Applications, ISSN:2319-7471, Vol. 4 Issue 9, September-2015.
5. Jaspreet Singh, Kartik Sharma, "*Energy efficient AODV routing protocol for mobile adhoc networks*", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 9, September2015, DOI: 10.17148/IJARCEE.2015.4928.121.
6. Krishna Chennakesava Rao M, Maheswar Vissa, Mrudula S, Ashutosh Kumar Dixit*," Energy Efficient Cluster based Routing Protocol for Wireless Sensor Networks*" IEEE-International Conference on Control, Instrumentation, Communication Computational Technologies (IEEE-ICCICCT 2015), December 2015. DOI: 10.1109/ICCICCT.2015.7475390
7. Reena Singh, Shilpa Gupta, "*EE-AODV: Energy Efficient AODV routing protocol by optimizing route selection process*", International Journal of Research in Computer and Communication Technology (IJRCCT), Vol. 3, Issue 1, January-2014.
8. Archan Misra, Suman Banerjee, "*MRPC:Maximizing Network Lifetime for Routing in Wireless Environments"*, IEEE Wireless Communications and Networking Conference (WCNC) 2002, March 2002.
9. G.Varaprasad*, "Power Aware and Signal Strength Based Routing Algorithm for Mobile AdHoc Networks*", 2011 International Conference on Communication Systems and Network Technologies, DOI: 10.1109/CSNT.2011.34.
10. Shivashankar, Hosahalli NarayanaGowda Suresh, Golla Varaprasad, Guruswamy Jayanthi, *"Designing Energy Routing Protocol with Power Consumption Optimization in MANET*", IEEE Transactions on Emerging Topics in Computing, October 2013, DOI: 10.1.09/TETC.2013.2287177.