Study of Energy Conservation & Security in MANET

Sunil Taneja[1] , Amandeep Makkar[2]

[1]Assistant Professor, Department of Computer Science, Govt. College, Aharwala, Bilaspur, Haryana, India

[2]Assistant Professor, Department of Computer Science, Arya Girls College, Ambala Cantt, Haryana, India

ABSTRACT

In this industrial revolution 4.0 i.e. Digital Revolution, wireless technology is going to be widely used for data communication. One of the widely used wireless technologies is Mobile Ad hoc Network (MANET). MANET comprises of movable nodes and these nodes communicate with other nodes until they remain in radio range of each other. MANET suffers from two main issues First, Various security attacks in MANET & privacy Issues in MANET Second, energy consumption. These two issues cumulatively deteriorate the performance of MANET. Therefore, improvement in various routing protocol is challenge for researchers to overcome security lacunas and energy efficiency. In this research paper effort has been made to overcome these challenges. Energy Aware Secure (EAS-AODV) routing algorithm based on AODV routing protocol has been proposed that will address both challenges in MANET and will enhance the reliability of the MANET. Network Simulator-2 has been used for simulation. Simulation results show that proposed technique provides a secure routing protocol that enhances the energy efficiency in MANET and makes MANET a more reliable network. The performance of network is analyzed in form of PDR, routing overhead, energy consumption, delay and hop count.

KEYWORDS: AODV, Energy, MANET, PDR, Routing, Security

ISBN: 978-81-955611-3-1

1. INTRODUCTION

One of the most important characteristic of MANET is its infrastructure-less system where nodes are self arranging. In MANET every node can interact with others without having any base station. Various mobile devices in mobile ad hoc networks comprises of limited resources for data communication such as limited radio range etc. In this way, a node can communicate with other active nodes present in the network for data communication. In MANET a node can serves three purpose sender, destination and intermediary node. So that during data communication a route may have different multi nodes. Routing is a significant issue in the MANET. Routing is a mechanism that helps in data communication between two nodes when they are not directly connected with each other or remain in the radio range of each other. For routing purpose there are numerous routing protocols present in MANET and these protocols are broadly classified into three categories. Proactive routing also called as table driven routing protocol. Reactive routing also known as On-demand protocols. And last is hybrid routing which is blend of both above said routing. On demand routing strategy establish route only when require & it is most widely use routing because this is more efficient than table driven. Most widely reactive routing protocol is Ad-hoc On-demand Distance Vector (AODV) routing. AODV uses various packets during data communication such as RREQ, RREP and RERR etc. Due to mobile nodes link breakage is very frequent leads to more routing process in network. More routing process consumes more energy of nodes leads to decline of reliability of MANET. This paper provides an enhanced algorithm for enhancing data communication.

Figure 1: Mobile Ad hoc Network

ISBN: 978-81-955611-3-1

2. Literature Review

Chitra et al. anticipated PPSEER(Privacy Protecting Secure and Energy Efficient Routing Protocol). Proposed scheme is an effort towards addressing the key challenges of security and energy conservation in MANET. For security operation author used encryption technique and this is based on group signature. Before executing encryption organization of different nodes in network take place based on their energy intensity. Encryption technique also includes other secure parameters like maximum transmission power and secret key and these parameters are only known to sender and receiver node. When comparing it with existing algorithm author found that it enhanced the privacy of message and it maintains energy efficiency of nodes.

Arya et al. proposed modified algorithm with base protocol AODV that ensure more energy efficiency and security. In planned algorithm, every node in the network set itself as an immoral node on the basis of various flag values and this is done to test out the nasty behavior of adjacent nodes. After that energy efficiency is performed and for this the route is formed locally by use of those adjacent nodes of the upstream nodes which have the maximum energy intensity.

S. Kumar et al. projected a stability and Energy Aware Reverse Adhoc On demand Distance Vector (SEAR-AODV) Routing protocol. The proposed work is based on the enhancement of the existing routing protocol based on AODV i.e. R-AODV. Optimization in proposed algorithm is performed by computing the reliability factor (RF) of various nodes which includes two performance metrics energy and route stability. After computation of RF value proposed algorithm choose the path with high RF value for data communication. Other secondary and tertiary paths are used on the basis of descending order of their RF score. It uses a new make-before- break route maintenance mechanism.

Phu et al. proposed a secure AODV routing protocol for MANET. In order to make AODV more secure author used secure schema strategy in MANET & every node in this schema strategy hold a list of neighboring nodes with secret that is mined by performing a key concord when unification of a network. Prime principal of this schema is that for ensuring the non repudiation and integrity of the network each node in the network performs

ISBN: 978-81-955611-3-1

message authenticated process with the sender node before initiating route discovery process. So that it could prevent the network from attacks from malicious nodes. When compared it with existing algorithm proposed scheme requires less power in routing and provides more security.

3. Proposed Scheme

On the basis of literature review, various gaps have been identified in MANET routing. Primarily, two important gaps are Security of network and energy conservation in MANET. In this research work, an algorithm has been proposed to address these challenges. In the direction of accomplish the purpose, an Energy Aware Secure AODV (EAS-AODV) protocol is projected. For security of the network, asymmetric cryptography technique has been used. For energy conservation, a mechanism has been devised i.e. when path set downs throughout communication upstream node initiates local route request (LRREQ) to its whole adjacent node as a substitute of generating RRER message & adjacent nodes respond with RREP with its energy values.

STEP BY STEP PROCEDURE

1. Sender initiates RREQ with its certificate
2. If current energy level of node is greater than threshold then node is selected for route formation.
3. Else, Upstream node initiate local route request(LRREQ)
4. Adjacent node receives RREQ & if neighbor node is itself destination throw RREP to source

   Else advance RREQ to its bordering nodes until destination is reached
5. If (destination decrypt the certificate & get IP, public key of sender and time stamp)

   It verifies sender node as legitimate node Else RREQ is originated by malicious node
6. Destination initiates RREP with a range of routes accessible to it.
7. Total energy of each path is divided by its equivalent hop count & imagines that x comes out. The path with maximum value of x is chosen.

ISBN: 978-81-955611-3-1

4. SIMULATION ENVIRONMENT

The following parameters have been used while carrying out simulation over NS-2:-

Parameter	Values
Routing Protocol	SEAR- AODV, EAS-AODV
No. of Nodes	10,20,30,40,50,75
Terrain Area	1000mX1000m
Simulation Time	100.0sec
Packet Size	512bytes
Maximum Speed of nodes	2,5,10,25,50,75 m/s
Transmission Range	250m
No of Flows	10
Frequency Band	2.4 GHz
Propagation Type	Propagation/ TwoRayGround
Queue Type	Queue/Drop Trail/PriQueue
Mobility Model	Random Waypoint
Nodes' Initial Energy	100 J
S Thr2	1.5×R×Thr
S Thr1	1.5×R×Thr
Pause Time	2 sec
Queue Length	50
MAC Type	Mac/802_11b
Antenna	Antenna/Omni Antenna
Traffic Type	CBR
Bandwidth	2.0 Mbps
Transmission Rate	4 Packets/ Sec

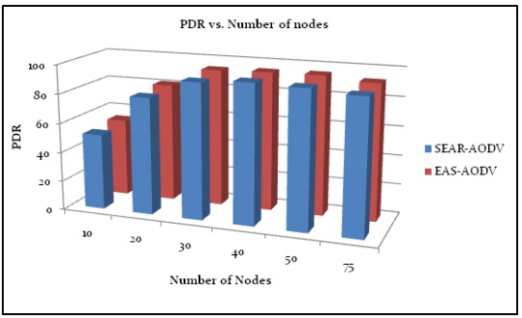

Figure 2: PDR vs. Number of nodes

ISBN: 978-81-955611-3-1

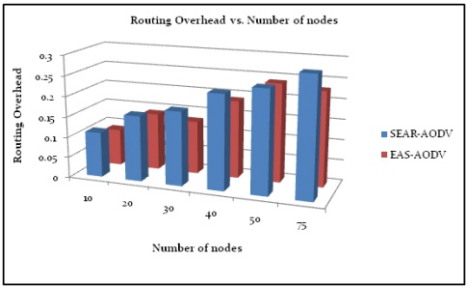

Figure 3: Routing Overhead vs. Number of nodes

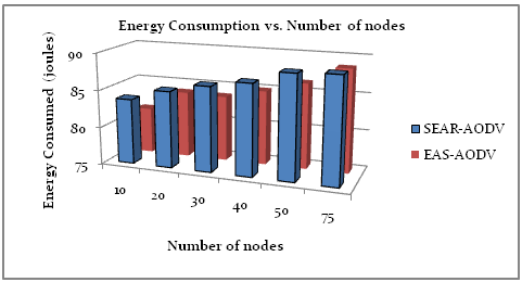

Figure 4: Energy Consumption vs. Number of nodes

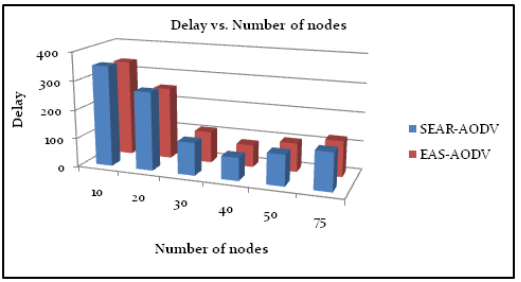

Figure 5: Delay vs. Number of nodes

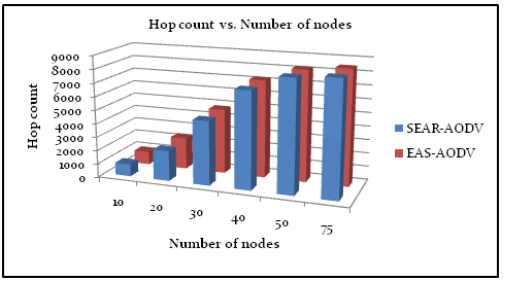

Figure 6: Hop Count vs. Number of nodes

ISBN: 978-81-955611-3-1

It can be easily inferred from the above figures that the projected algorithm is extra consistent than traditional routing protocol. Performance has been done on various performance metrics & analyzed that proposed algorithm i.e. Energy Aware Secure AODV outperforms the existing algorithm. Figure 2 provides Comparison of PDR with respect to number of nodes. It is clear from the figure that EAS-AODV gives better PDR than SEAR-AODV routing protocol. Figure 3 & Figure 4 provides comparison of routing overhead and energy consumption during data communication respectively. As results are analyzed it shows that the proposed algorithm performs better as compared to existing one. Figure 5 & Figure 6 provides comparison of end to end delay and hop count during data transmission. On these metrics, the proposed algorithm also outperforms the traditional algorithm. Overall performance of the proposed EAS-AODV protocol is better than the existing routing protocol.

5. CONCLUSION AND FUTURE SCOPE

The motto behind this research paper is to develop an algorithm that addresses the challenges of energy conservation and security. It is clear from the above figures that the research work carried out is able to address these issue up to a large extent and with over algorithm traditional AODV performance better in terms of various parameters. But due to increasing cyber threats and various issues, there are immense potential for further modification in AODV. Total optimization of the AODV in term of energy efficiency and various other parameters is yet to achieve. So the future researches can be made to make AODV more reliable and authenticated.

6. BIBLIOGRAPHY

[1] Dorri et al., "Security Challenges in Mobile Ad Hoc Networks: A Survey", International Journal of Computer Science & Engineering Survey, 2015, 6(1), pp. 15-29.

[2] S. Yadav et al., "Securing AODV routing protocol against black hole attack in MANET using outlier detection scheme", Proceedings of 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics, 2017, pp. 1–4.

[3] N. Gupta et al., "Performance Evaluation of DSR , AODV and SAODV Routing Protocol in MANETs", International Journal on

Future Revolution in Computer Science & Communication Engineering, 2018, 4(3), pp. 151-161.

[4] U. Rashid et al., "Mobility and energy aware routing algorithm for mobile ad-hoc networks", Proceedings of International Conference on Electrical Engineering, 2017, pp. 1–5.

[5] E. Niewiadomska-Szynkiewicz et al., "Secure low energy AODV protocol for wireless sensor networks", Proceedings of 27th International Telecommunication Networks Application Conference ITNAC, 2017, pp. 1–6.

[6] N. Kamboj et al., "An Enhanced Energy Efficient Secure Routing Protocol for MANET", International Journal of Advanced Science and Technology, 2020, 29(5), pp. 1135–1142.

[7] Eenavath Veeraiah et al., “Trust Aware Secure Energy Efficient Hybrid Protocol for MANET”, IEEE Access Multidisciplinary Open Access Journal, 2021, Volume 9, pp. 120996-121005.

ISBN: 978-81-955611-3-1